Ubee DDW3611 Wireless Cable Modem Gateway

Firmware Version: 8.6.4012D2

Subscriber User Guide

www.ubeeinteractive.com
8085 S. Chester Street, Suite 200
Englewood, CO 80112
1.888.390.8233
Sales (email): amsales@ubeeinteractive.com
Support (email) amsupport@ubeeinteractive.com

November 2012

Notices and Copyrights

This device is Wi-Fi Alliance Certified.

www.ubeeinteractive.com
8085 S. Chester Street, Suite 200
Englewood, CO 80112
1.888.390.8233
Sales (email): amsales@ubeeinteractive.com
Support (email) amsupport@ubeeinteractive.com

November 2012

Contents

1 Introduction

Welcome to the Ubee family of data networking products. This guide is specific to the Ubee DDW3611 Wireless Cable Modem Gateway and serves the following purposes:

- Provides multiple system operators (MSOs) for cable systems with the information necessary to operationally stage, deploy, and support the DDW3611.
- Provides the technical details needed to locally and remotely manage deployed devices. This can involve setting up configuration files, downloading the files to the device, and obtaining information from the device for support and troubleshooting.
- Defines all relevant device compliance standards and physical specifications.
- Provides information used by the following MSO entities:
  - Office of the CTO
  - Procurement, Network Engineering, and Test Organizations
  - Physical and Environmental Engineers
  - Technical Operations
  - Installation and Repair
  - Customer Care
  - Training Organizations
- Provides installation instructions and device Web interface instructions to configure and manage the device.

Topics

See the following topics:

1.1 Understanding Safety and Regulatory Information

The following information provides safety and regulatory standards to install, maintain, and use the DDW3611 Wireless Modem Gateway.

1.1.1 Understanding Safety

WARNING: The following information provides safety guidelines for anyone installing and maintaining the DDW3611. Read all safety instructions in this guide before attempting to unpack, install, operate, or connect power to this product. Follow all instruction labels on the device itself. Comply with the following safety guidelines for proper operation of the device:

Always follow basic safety precautions to reduce the risk of fire, electrical shock, and injury. To prevent fire or shock hazard, do not expose the unit to rain, moisture, or install this product near water. Never spill any form of liquid on or into this product. Do not use liquid cleaners or aerosol cleaners on or close to the product. Use a soft dry cloth for cleaning.

Do not insert any sharp object into the product's module openings or empty slots. Doing so can accidentally damage its parts and/or cause electric shock.

Electrostatic discharge (ESD) can permanently damage semiconductor devices. Always follow ESD-prevention guidelines for equipment handling and storage.

Use only the power adaptor supplied with the device. Do not attach the power supply cable to building surfaces or floorings.

- ❑ Rest the power cable freely without any obstacles. Do not place heavy items on top of the power cable. Refrain from abusing, stepping or walking on the cable.
- ❑ Do not place heavy objects on top of the device. Do not place the device on an unstable stand or table; the device can drop and become damaged.
- ❑ To protect the equipment from overheating, do not block the slots and openings in the module housing that provide ventilation. Do not expose this device to direct sunlight. Do not place any hot devices close to this device, as it may degrade or cause damage to it.

1.1.2 Understanding Eco-Environmental Statements

The following eco-environmental statements apply to the DDW3611.

Packaging Collection and Recovery Requirements:

Countries, states, localities, or other jurisdictions may require that systems be established for the return and/or collection of packaging waste from the consumer, or other end user, or from the waste stream. Additionally, reuse, recovery, and/or recycling targets for the return and/or collection of the packaging waste can be established. For more information regarding collection and recovery of packaging and packaging waste within specific jurisdictions, contact Ubee Interactive at www.ubeeinteractive.com.

1.1.3 Understanding Regulatory Statements

The following regulatory statements apply to the DDW3611.

Industry North America Statement:

This device complies with RSS-210 of the Industry North America Rules. Operation is subject to the following two conditions:

(1) This device may not cause harmful interference.

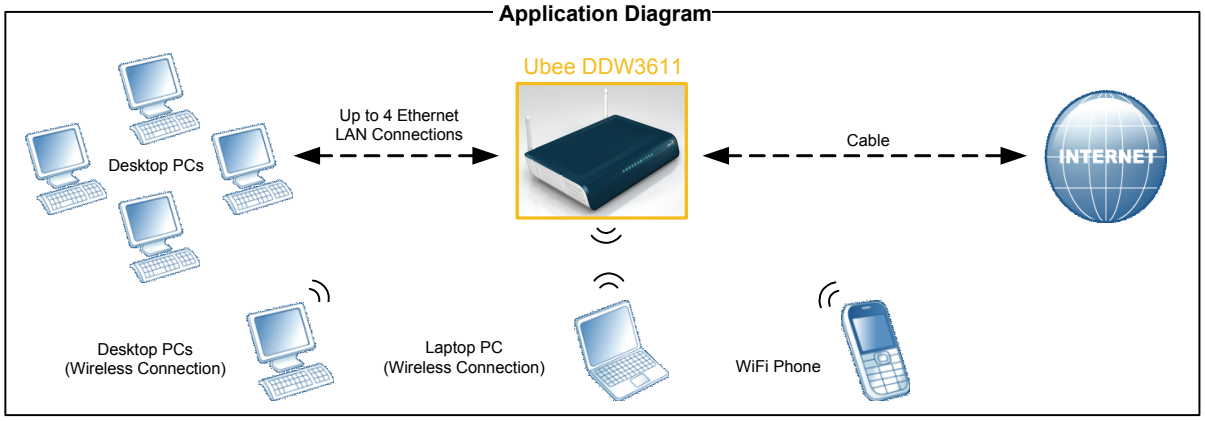
(2) This device must accept any interference received, including interference that may cause undesired operation.

Radiation Exposure Statement:

This device complies with FCC radiation exposure limits set forth for an uncontrolled environment and should be installed and operated with a minimum distance of 20cm between the radiator & your body. This device has been designed to operate with an antenna having a maximum gain of 2 dBi. Antenna having a higher gain is strictly prohibited per regulations of Industry North America. The required antenna impedance is 50 ohms.

1.2 Understanding Connections and Applications

The following diagram illustrates the general connection topology and applications of the DDW3611.



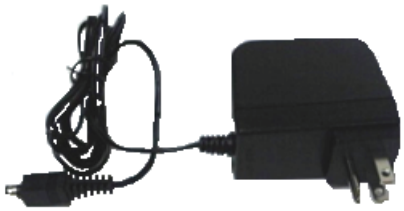
1.3 Requesting Support

Subscribers must contact their service provider for direct support. Device documentation support may be available at:

http://www.ubeeinteractive.com

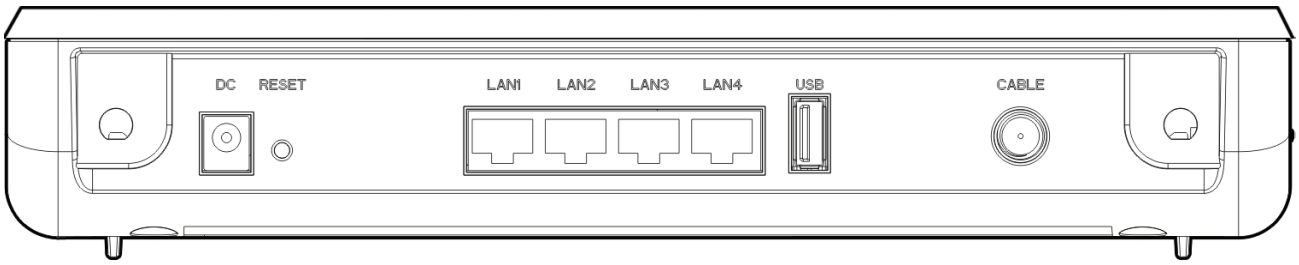
1.4 Checking Device Package Components

The package for the DDW3611 contains the following items:

Item	Description
	1 - RJ45 Ethernet Cable 6.0 ft RoHS & UL compliant Sample image, actual appearance subject to change.
	1 - Power Supply: Use only a 12V/1.5A Sample image, actual appearance subject to change.
	2 - Antennas: White wireless network antennas Sample image, actual appearance subject to change.

1.5 Understanding the Device Rear Panel

Review the following image and descriptions of the rear panel connections on the device.



Item	Description
DC	Connects the power adaptor to the device. Use only the power adaptor provided with the DDW3611.
RESET	Restores the default settings of the device including wireless and custom gateway settings. Use a pointed object to push down the reset button for 5-10 seconds until the power LED turns off. After the power LED turns off, release the button.
LAN1 **LAN2** **LAN3** **LAN4**	Connects the device to local area network (LAN) Ethernet devices such as computers, gaming consoles, and/or routers/hubs using an RJ45 cable. Each LAN port on the back panel of the device has an LED on the front of the device to indicate its status when an Ethernet device is connected. When an Ethernet device is connected to the cable modem: ♦ LED is **Green** when connected at 10/100 Mbps speeds. ♦ LED is **Blue** when connected at 100/1000 speeds (Gigabit Ethernet). ♦ LED blinks when data is passed between the cable modem and the connected device.
USB	Connects to some USB devices, such as computers and flash drives if the USB connector is supported/enabled by the service provider.
CABLE	Connects to the cable outlet (with the cable provided by your service provider), or a cable splitter connected to the cable outlet.
WPS	Connects a PIN-protected Wi-Fi device to the cable modem when the Wi-Fi Protected Setup method is used. When the WPS button is pushed or triggered through the device's Web GUI, an LED on the front of the device blinks for four minutes until a PIN is entered from the wireless client, such as a laptop computer, that wants to connect. After a Wi-Fi client attaches successfully, the LED remains on for five minutes, and then turns off. Refer to Understanding the Wireless Menu on page 57 for more information.

1.6 Understanding Specifications, Standards, and Firmware

The following list provides the features and specifications of the DDW3611.

Interfaces

- Cable: F-Connector, Female
- LAN: 4 10/100/1000 Mbps RJ45 Ports
- USB: 1 USB 2.0 HOST Port (USB port is powered, but is not activated for subscriber use. It is NOT a USB Client port, so it cannot be used for Internet access.)
- Wireless: 802.11a/b/g/n, 2.4GHz or 5GHz (Simultaneous dual band not supported.)

Standards/Certifications

- DOCSIS 3.0/Euro DOCSIS 3.0 Certified
- DOCSIS/Euro DOCSIS 1.0/1.1/2.0 Certified
- Wi-Fi Alliance Compliant
- CE/FCC Class B

Downstream*

- Frequency Range: 88MHz ~ 1002MHZ
- Modulation: 64 / 256 QAM, Channel B/W: 6 MHz
- Maximum Data Rate per Channel (up to 8 channels):
- DOCSIS = 30 Mbps (64 QAM), 42 Mbps (256 QAM), EuroDOCSIS = 41 Mbps (64 QAM), 55 Mbps (256 QAM)
- Total Max Bandwidth (8 Channels): DOCSIS = 343 (304) Mbps, EuroDOCSIS 444 (400) Mbps
- Symbol Rate: 6952 Ksps
- RF Input Power: -15 to +15dBmV (64 QAM), -15 to +15dBmV (256 QAM)
- Input Impedance: 75 Ω

Upstream*

- Frequency Range: 5MHz ~ 65MHz
- Modulation A-TDMA: QPSK, 8, 16, 32, 64QAM, S-CMDA: QPSK, 8, 16, 32, 64, 128QAM
- Max B/W of 4 Channels = 122.88 (108) Mbps, B/W Per Channel (up to 4 channels) = [QPSK 0.32 ~ 10.24 Mbps, 8 QAM 0.48 ~ 15.36 Mbps,
  16 QAM 0.64 ~ 20.48 Mbps, 32 QAM 0.80 ~ 25.60 Mbps,
  64 QAM 0.96 ~ 30.72 Mbps, 128 QAM/TCM 30.72 Mbps]
- Symbol Rate: 160, 320, 640, 1280, 2560, 5120 Ksps
- RF Output Power: TDMA/ATDMA: +8dBmV to +54dBmV (32/64 QAM). ATDMA Only: +8dBmV to +55dBmV (8/16 QAM), +8dBmV to +58dBmV (QPSK). S-CDMA: +8dBmV to +53dBmV (all modulations)

*Actual speeds vary based on factors including network configuration and speed.

Security

- VPN Pass-Through (IPSec/L2TP/PPTP)
- NAT Firewall, MAC/IP/Port Filtering, Parental Control
  - 1 DMZ Host supported
  - 252 DHCP Private IP Hosts supported by default.
- Stateful Packet Inspection (SPI), DoS Attack Protection
- WPS/ WPA/ WPA2/ WPA-PSK& 64/128-bit WEP Encryption (Default: WPA2-PSK)
- TACACS or RADIUS Authentication

Wireless and Network

- Supports 4 SSIDs, 802.11b/g/n compliant with speeds up to 300 Mbps (2 transmit, x 2 receive antennas)
- DHCP Client/Server / Static IP network assignment
- RIPv1/ v2
- Ethernet 10/100/1000 BaseT/full-duplex auto-negotiate functionality, IPv4 to IPv6 support.

Device Management

- Customer premises equipment (CPE)
- Supports IEEE 802.11e Wi-Fi Multimedia (WMM) and UAPSD (power savings)
- Web-Based Configuration
- Telnet Remote Management
- Secure Firmware Upgrade via TFTP
- Configuration Backup and Restore
- SNMP Support
- Interoperability with main CMTS products

Physical and Environmental

- Dimensions: 6.77” (172.2mm) x 10” (254mm) x 1.65” (42mm)
- Weight: 1.1 pounds (500 grams)
- Power: 12V/1.5A switching power supply
- Operating Temperature: 32°F ~ 104°F (0°C ~ 40°C)
- Humidity: 5 ~ 90% (non-condensing)

1.7 Understanding Default Values and Logins

The DDW3611 is pre-configured with the following parameters:

Local Port Address: 192.168.100.1, Web Interface: http://192.168.100.1

Operation Mode: NAT Mode

Subnet Mask: 255.255.255.0

Wireless Defaults:

- Primary SSID (subscriber-managed) = DDW3611 plus last 2 characters of the cable modem's MAC address with letters entered in upper case.

  Example: **DDW361184**

Notes:

- ❖ If the subscriber changes the SSID, the device does not revert to this default SSID when the device is reset, except when a manual reset is performed through the Web GUI (see Understanding the Tools Menu on page 81).
- ❖ The MAC address can be found on the device label or it can be found by opening an Internet browser window to the device. Refer to Using the Information Option on page 21 for instructions.

- Encryption Method = **WPA2-PSK** with **AES** encryption
- WPA Pre-shared Key = DDW3611 plus the last 6 characters (3 octets) of the cable modem's MAC address (UPPER case, if letters).

  Example: **DDW3611E44284**
- WPS PIN = Randomly generated eight digit number
- Device Name: **UbeeAP**

❑ **Standard User/Consumer Web Interface Login**:

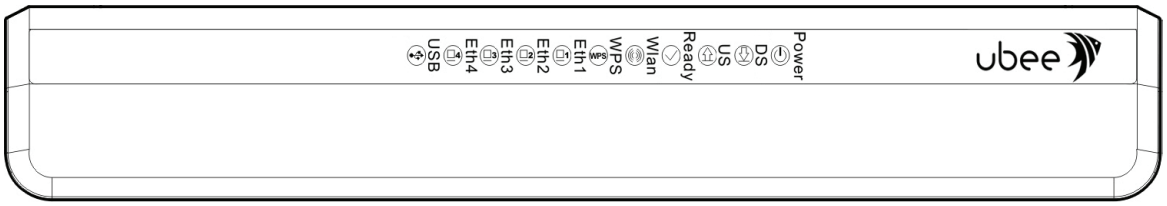
Username: **user**
Password: **user**

1.8 Understanding LED Operations

The following section describes what the device LEDs indicate.

1.8.1 Understanding the Device Front Panel

The following image represents the front panel of the device. LED descriptions are provided in the following table.



1.8.2 Understanding LED Behavior

The following table summarizes the LED behavior of the DDW3611.

LED Color			Green	Green/ Blue	Green/ Blue	Green/ Blue	Green/ Blue	Green	Green	Green	Green/ Blue	Green/ Blue	Green
LED Label			USB	Eth-4	Eth-3	Eth-2	Eth-1	WPS	Wlan	Ready	US	DS	Power
CM Initialization	1	Power on	On	On	On	On	On	Off	Off	On	On	On	On
	2	Load Image	Off	On if connected	On if connected	On if connected	On if connected	Off	Off	Off	Off	Off	Off
	3	H/W Check	Off	On if connected	On if connected	On if connected	On if connected	Off	On	Blinks	Blinks	Blinks	On
	4	DS Locked and Sync OK	Off	On if connected	On if connected	On if connected	On if connected	Off	On	Blinks	Blinks	On Green if 1 DS locked Blue if DS channel bonding	On
	5	US Ranging	Off	On if connected	On if connected	On if connected	On if connected	Off	On	Blinks	Blinks	On Green if 1 DS locked Blue if DS channel bonding	On
	6	US Ranging OK	Off	On if connected	On if connected	On if connected	On if connected	Off	On	Blinks	On Green if 1 US locked Blue if US channel bonding	On Green if 1 DS locked Blue if DS channel bonding	On
	7	Registration OK	Off	On if connected	On if connected	On if connected	On if connected	Off	On	On	On Green if 1 US locked Blue if US channel bonding	On Green if 1 DS locked Blue if DS channel bonding	On
	8	NACO Enable (network access)	Off	On if connected	On if connected	On if connected	On if connected	Off	On	On	On Green if 1 US locked Blue if US channel bonding	On Green if 1 DS locked Blue if DS channel bonding	On
	9	NACO Disable	Off	On if connected	On if connected	On if connected	On if connected	Off	On	Off	On Green if 1 US locked Blue if US channel bonding	On Green if 1 DS locked Blue if DS channel bonding	On
CM Operation	1	Attached CPE	On Green	On Green if connected Blue if speed linked at 1000Mbps (GigE)	On Green if connected Blue if speed linked at 1000Mbps (GigE)	On Green if connected Blue if speed linked at 1000Mbps (GigE)	On Green if connected Blue if speed linked at 1000Mbps (GigE)	On	On	On	On Green if 1 US locked Blue if US channel bonding	On Green if 1 DS locked Blue if DS channel bonding	On
	2	CPE Data Tx/Rx	Blinks	Blinks if connected	Blinks if connected	Blinks if connected	Blinks if connected	Blinks	Blinks	On	On Green if 1 US locked Blue if US channel bonding	On Green if 1 DS locked Blue if DS channel bonding	On

2 Installing the DDW3611

This chapter describes how to set up and connect the DDW3611, connect additional devices, and troubleshoot the installation.

Topics

See the following topics:

2.1 Setting Up and Connecting the DDW3611

Use the following instructions to set up and connect the DDW3611. When the device is set up and connected, refer to Accessing the Web Interface on page 17 to configure the device.

Important: Subscribers contact your service provider to enable Internet access and wireless networking.

Typically, the service provider initially configures and connects the device. The installation steps are provided below if you wish to confirm the setup or add devices to your network. Refer to Connecting Devices to the Network on page 12.

Steps

To set up the device:

1. Remove the contents from the device packaging.
2. Place the DDW3611 in the best location to connect to other devices, such as PCs or gaming consoles.
   - Place the wireless cable modem and wireless clients in open areas far away from transformers, heavy-duty motors, microwave ovens, refrigerators, fluorescent lights, and other manufacturing equipment. These items can impact wireless signals. A wireless signal can become weaker after it has passed through metal, concrete, brick, walls, or floors.
   - Place the device in a location that has an operating temperature of 0˚ C to 40˚ C (32˚ F to 104˚ F). Refer to Understanding Safety and Regulatory Information on page 1 for more safety information.
3. Power on your PC. The PC must have an Ethernet network adaptor or Ethernet port and an Internet browser installed, such as Netscape or Internet Explorer. The following browsers are supported:
   - For Windows 2000, XP, Vista, Windows 7, Firefox 1.07 and higher, Internet Explorer v7 and above, Netscape.
   - For MAC OS X, 10.2, and higher: Firefox 1.07 and higher, Safari 1.x and higher.
4. Connect the power cord included in the product package to the back of the cable

modem and then to the power outlet.

5. Connect the network cable included in the product package to your computer's Ethernet port. Connect the other end to the LAN1, LAN2, LAN3, or LAN4 port to the cable modem.
6. Connect a coaxial cable from the CABLE port on the device to the cable wall outlet, or to a cable splitter connected to the wall outlet.
7. Connect the two antennas provided in the product packaging.
8. Validate the network connection using the device LEDs to confirm operations:
   - The Wlan LED must be solidly lit.
   - The Power, DS, US, and Ready LEDs are solidly lit.

   Refer to Understanding LED Operations on page 8 for more information.

2.2 Connecting Devices to the Network

Use the instructions below to connect network devices and validate device functionality.

Topics

See the following topics:

2.2.1 Connecting an Ethernet Device

You can connect up to three additional Ethernet devices to the DDW3611.

Steps

To connect another Ethernet device to the network:

1. Connect the Ethernet cable from the Ethernet device (for example, a PC or gaming console) to an open Ethernet port on the back of the DDW3611.
2. Use the device LEDs to confirm operations. Refer to Understanding LED Operations on page 8 for more information.
3. Open a Web browser and go to any Web site to validate network/Internet connectivity (for example, http://www.wikipedia.org).
4. If the connected device is a gaming console, perform any online task supported by the console (for example, log into the gaming server, play an online game, download content).

Refer to Troubleshooting the Installation on page 14 for troubleshooting information.

2.2.2 Connecting a Wireless Device

Use the following steps to connect a wireless device to the DDW3611 (for example, a laptop computer).

Steps

To connect a wireless device:

1. Access the wireless networking feature on your wireless device. On a Windows computer, for example, double-click the **Wireless Network Connection** icon in the system tray (lower-right side of the Windows desktop).
2. Click **View Wireless Networks**. The device is shipped with a default SSID. The SSID is the name of the wireless network broadcast from the device so that wireless clients can connect to it.
3. Double-click your **SSID** in the wireless networks window. The default SSID is the device name DDW3611 plus the last 2 characters of the cable modem's MAC address, with letters entered in upper case.

   Example: **DDW361184**

   Notes: You can find the MAC address on the device label or by opening an Internet browser window to the device. Refer to Using the Information Option on page 21 for instructions. If the subscriber changes the SSID, the device does not revert to this default SSID upon any reset of the device, except in the case of a manual reset using the device's Web user interface. See Understanding the Tools Menu on page 81.

   When prompted, enter the Network Key, which is the device name (DDW3611) plus the last 6 characters (3 octets) of the cable modem's MAC address (UPPER case, if letters).

   Example: **DDW3611E44284**

   - If using WPS, enter the WPS personal identification number (PIN). The WPS PIN is a randomly-generated number found on the Wireless Primary Network screen. Refer to Using the Primary Network Option on page 61.

   WPA-WPA2 AES is the default encryption method.
4. Confirm connectivity by opening a Web browser and going to any Web site (for example, http://www.wikipedia.org) or access the Web interface for the DDW3611.

Note

The Web interface allows you to customize the configurations and capabilities for the device. For a full explanation of all Web interface functions, refer to Using the Web User Interface on page 17.

If you are having wireless issues or questions, refer to on page 66.

2.2.3 Connecting a USB Device

You can connect to some USB devices, such as computers and flash drives, if the USB connector is supported/enabled by the service provider.

You must **contact your service provider** to have the USB port enabled.

Steps

To connect a USB device:

1. Connect a USB cable to the USB port on the back panel of device.
2. Connect the other end of the USB cable to the USB device.
3. Access the USB device. Access depends on the type of device connected.

2.3 Troubleshooting the Installation

Use the following tips to troubleshoot the installation.

- **None of the LEDs are on when I power on the DDW3611.**
  - Verify the power outlet is energized and the power adaptor is connected to the power outlet.
  - Check the connection between the power adaptor and the cable modem. Power off the cable modem and wait for 5 seconds and power on the modem again. If the problem still exists, there may be a hardware problem.
- **The LAN1, 2, 3, or 4 LEDs are not lit where Ethernet cables are connected.**
  - Restart the computer so that it can re-establish a connection with the cable modem.
  - Check for a resource conflict (Windows users only):
    1. Right-click the **My Computer** icon on your desktop and choose **Properties**.
    2. Choose the **Device Manager** tab and look for a yellow exclamation point or red X over the network interface card (NIC) in the Network adaptors field. If you see either one, you may have an interrupt request (IRQ) conflict. Refer to the manufacturer's documentation or your service provider for further assistance.
  - Verify that TCP/IP is the default protocol for your network interface card.
  - Power cycle the cable modem by removing the power adaptor from the electrical outlet and plugging it back in. Wait several minutes for the cable modem to re-establish communications with your cable service provider.

❑ Check General Connectivity Issues:

- If your PC is connected to a hub or gateway, try connecting the PC directly into an Ethernet port on the cable modem.
- If you are using a cable splitter, try removing the splitter and connecting the cable modem directly to the cable wall outlet. Wait several minutes for the cable modem to re-establish communications with your cable service provider.
- The Ethernet cable may be damaged. Try another cable.

3 Using the Web User Interface

The user interface for the DDW3611 is easy to use and allows you to view and configure several settings for your wireless gateway device. You can also validate the installation by accessing the Web user interface on the device.

Understanding Operation Modes and the Web User Interface on page 19.

Topics

See the following topics:

3.1 Accessing the Web Interface

Access the Web user interface for the DDW3611 from a Web browser, such as Internet Explorer, from a computer.

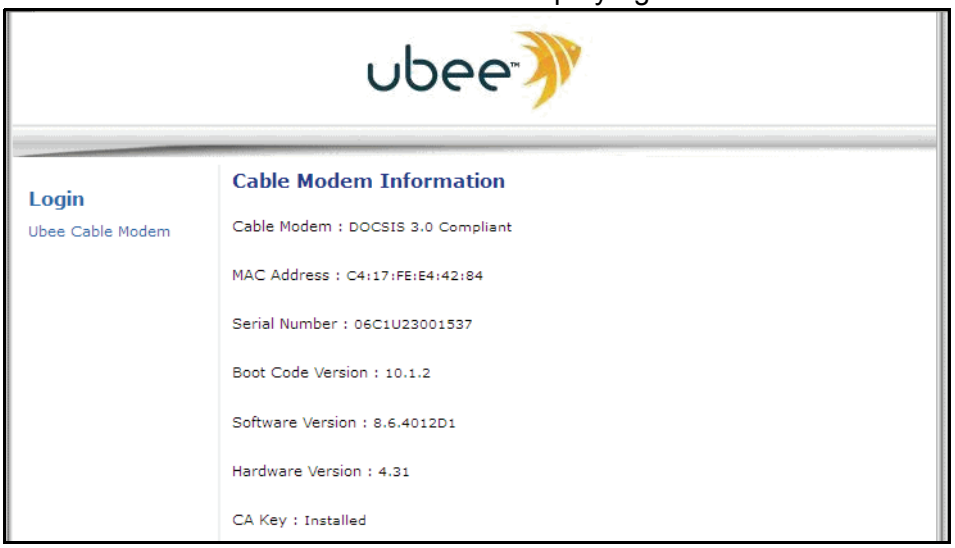
Steps

To access the Web user interface:

1. Launch an Internet browser, such as Internet Explorer, from your computer.
2. Enter the following IP address in the address bar of the browser window and press <**Enter**>.

   `http://192.168.100.1`

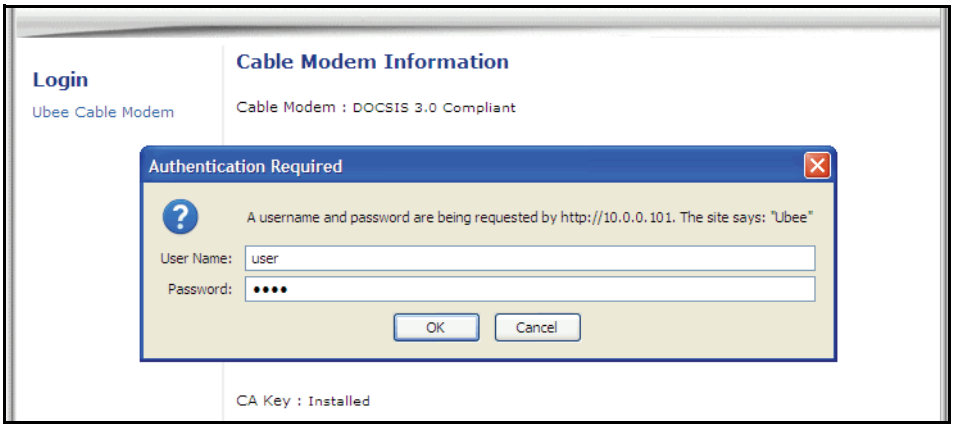
   The Cable Modem Information screen displays general modem information.



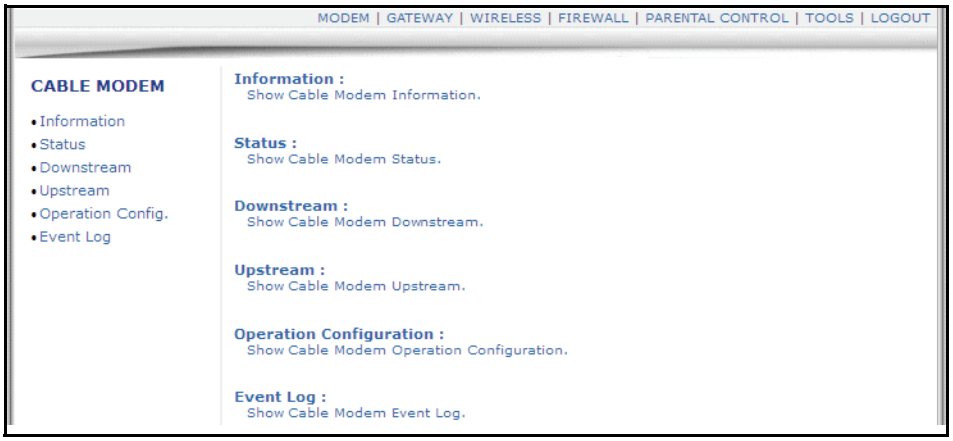
3. Click **Login** on the left side menu to access the Web interface.

4. At the login window, enter the user credentials.
   - Standard subscriber Web interface login (all lower case letters):

     Username: **user**
     Password: **user**



5. Click **OK**. The Cable Modem screen of the Web interface is displayed.



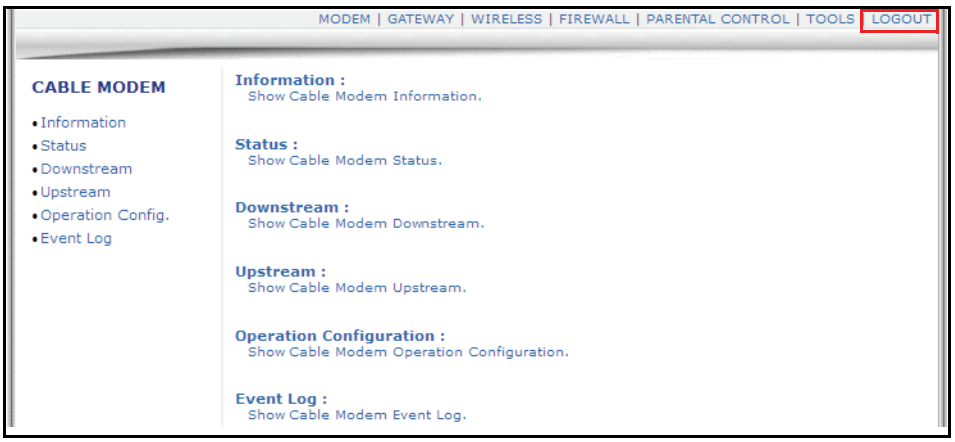
3.2 Logging Out of the Web Interface

Log out when finished using the Web user interface.

Steps

To log out of the user interface:

1. Click **Logout** from the main menu.



The logout screen is displayed.

2. Click **Back to Login** to access the Login screen and begin a new user interface session.

3.3 Understanding Operation Modes and the Web User Interface

The DDW3611 provides four operation modes. Different options are available in the Web user interface depending on the mode and the type of user logged in. The operation mode is set from the Tools menu Operation Mode option.

Bridge

Provides a wireless side for a specific access point. Enables layer 2 protocols, in which (usually) one Public IP address is automatically assigned to the subscriber from the cable company's DHCP servers. In this mode, the first device to connect to a LAN or Wireless LAN interface gets the Public IP. Hint: Disable the wireless primary network SSID to ensure that only an Ethernet-based device (e.g., Home Router) gets the Public IP.

NAT

Provides a wireless access point that allows sharing a single Internet connection. Enables Layer 3 IP protocol, DHCP for private IP address assignment, NAT for network address and port translation, IP routing, firewall protection, and parental control features. Hint: All LAN and Wireless LAN interfaces are on the same Private IP subnet, and are translated to a single Public IP address on the WAN gateway interface to the Internet.

Router

Operates in Router Mode for assigning Static Public IP addresses with RIP when this mode is enabled. DHCP, Firewall, and NAT functionality are disabled by default. When Route Mode is enabled, you can configure the device from the Web User Interface (UI) Routing screen, or through the Telnet Command Line Interface (CLI). Refer to Using the Routing Setup Option on page 92 for more information.

NAT Router

Operates in NAT Router mode when enabled. Combines functionality found in both NAT and Router Modes. You can configure the device from the Web UI Routing screen or through the Telnet CLI. Refer to Using the Routing Setup Option on page 92 for more information.

Subscriber Web User Interface in Bridge Mode

Subscriber Web User Interface in NAT, Router, and NAT Router Modes

4 Understanding the Modem Menu

The **Modem** menu of the Web interface allows you to access information about the modem, such as status and battery information.

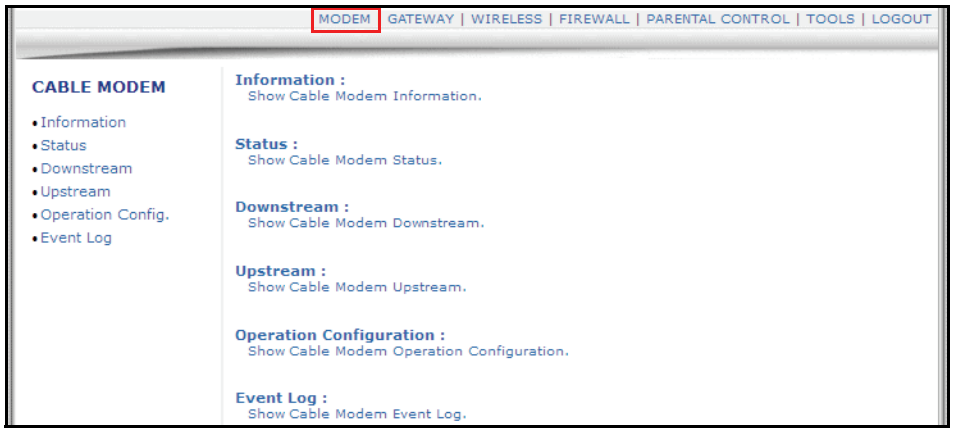
Topics

See the following topics:

Steps

To access modem options:

1. Access the Web interface. Refer to Accessing the Web Interface on page 17.
2. Click **Modem** from the main menu.



4.1 Using the Information Option

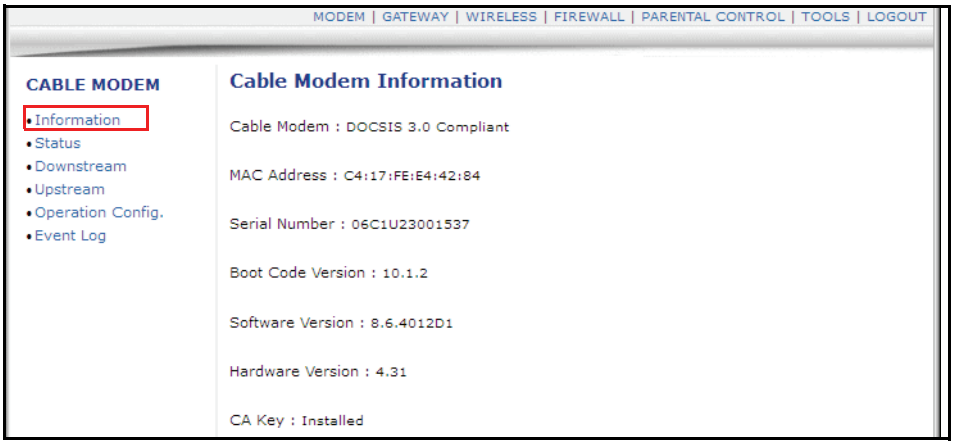
The **Information** option displays the device's internal software and hardware configuration.

Steps

To view modem information:

1. Click **Modem** from the main menu.
2. Click **Information** from the left side menu. Field descriptions are listed below the

screen example.



Label	Description
Cable Modem	Defines the current DOCSIS standard of the device.
MAC Address	Defines the unique media access control (MAC) hardware address of the cable modem.
Serial Number	Defines the unique manufacturer serial number of the device.
Boot Code Version	Defines the boot software code version of the device.
Software Version	Defines the general software version of the device.
Hardware Version	Defines the internal version number that identifies the hardware design.
CA Key	Defines the certificate authority (CA) key. The device installs a CA key that is transferred from the service provider's server after the cable modem is authenticated. The key is used to secure communication between the service provider and the cable modem.

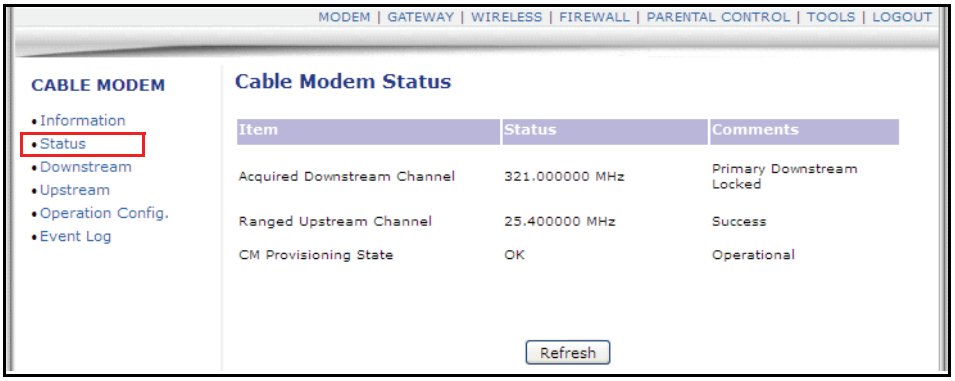
4.2 Using the Status Option

The **Status** screen displays the device's general connection information.

Steps

To view modem status:

1. Click **Modem** from the main menu.
2. Click **Status** from the left side menu. Field descriptions are listed below the following screen example.



Label	Description
Acquired Downstream Channel	Displays the Downstream channel tat the cable modem is trying to lock to and its progress.
Ranged Upstream Channel	Displays the Upstream channel the cable modem is trying to lock to and its progress.
CM Provisioning State	Indicates the state of the device, operational or otherwise (for example, In Progress, Disabled). After the physical initialization, the cable modem is configured by a DHCP server from the service provider. Once the cable modem obtains an IP address, the cable modem is online. The Status column shows the connection progress. The Comments column displays the messages indicating connection error information, if errors occur.

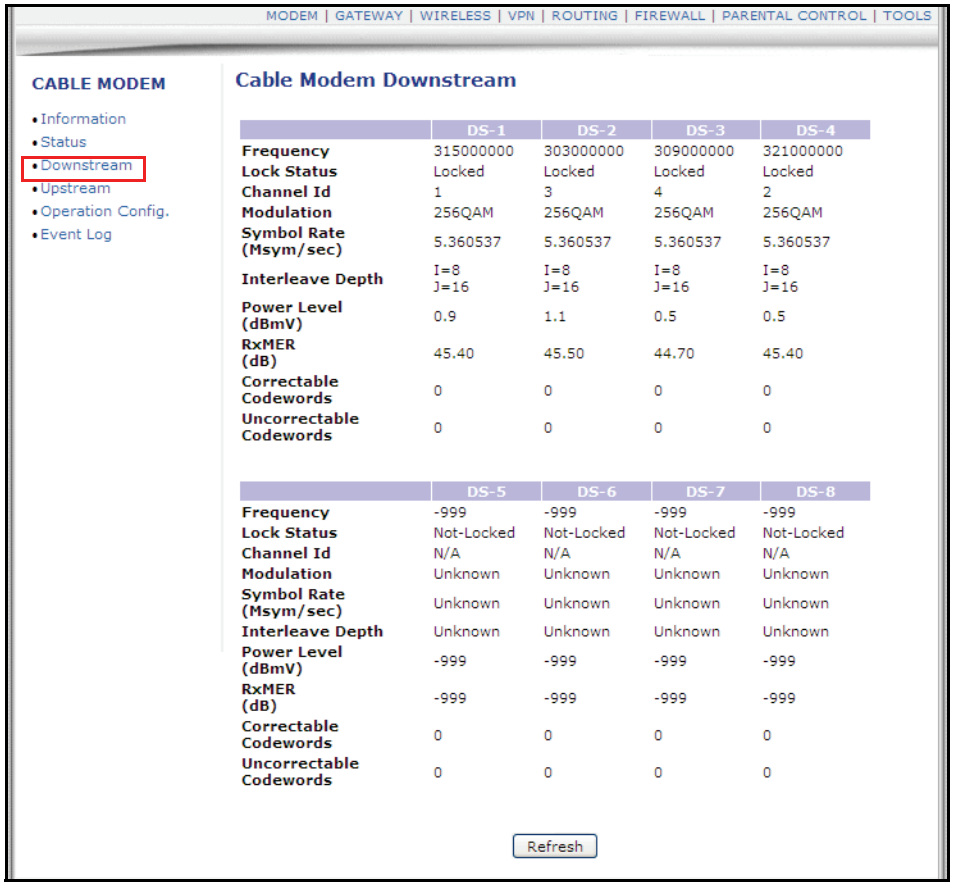
4.3 Using the Downstream Option

The **Downstream** screen displays detailed information on the network traffic from the service provider **to** the local computer (downstream channels).

Steps

To view downstream information:

1. Click **Modem** from the main menu.
2. Click **Downstream** from the left side menu. Field descriptions are listed below the following screen example.



Label	Description
DS-1 to DS-8	Numbers the downstream channels.
Frequency	Displays the downstream channel frequency on which the cable modem is scanning.
Lock Status	Displays if the cable modem succeeded in locking to a downstream channel.
Channel Id	Displays the downstream channel ID.
Modulation	Displays the modulation method required for the downstream channel to lock on to by the cable modem. This method is determined by the service provider.
Symbol Rate (Msym/sec)	Displays the symbol rate. Current cable modem downstream symbol rates: ♦ QAM64 is 5056941 sym/sec ♦ QAM256 is 5360537 sym/sec
Interleave Depth	Displays the current cable modem downstream Interleave depth (4/8/16/32/64/128/other).
Power Level (dBmV)	Displays the receiver power level in decibel millivolts after ranging process.

Label	Description
RxMER (dB)	Displays the Receiver Modulation Error Ratio used to quantify the performance of a digital radio receiver in a communications system using digital modulation.
Correctable Codewords	Displays the quantity of codewords which are correctable.
Uncorrectable Codewords	Displays the quantity of codewords which are not correctable.
Refresh	Updates the screen with the latest information.

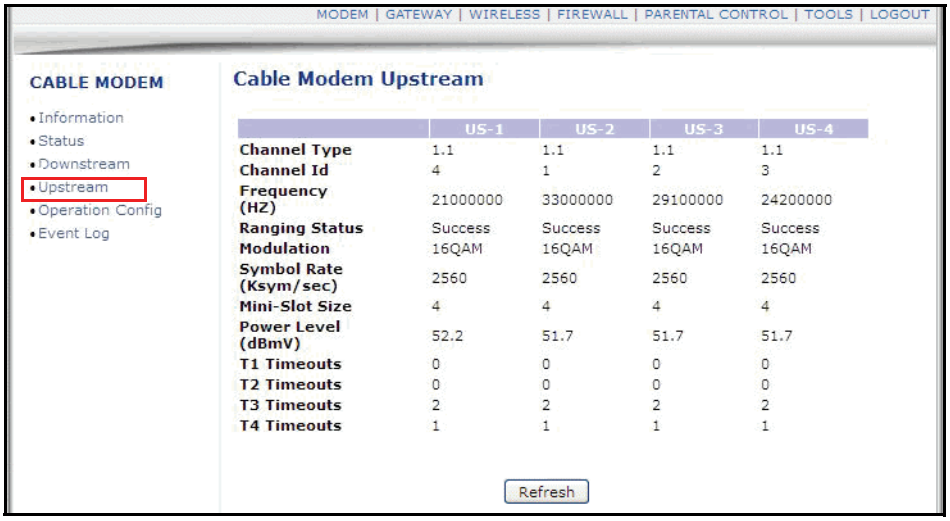
4.4 Using the Upstream Option

The **Upstream** screen displays detailed information on the network traffic **from** the computer to the remote destination (upstream channels).

Steps

To view upstream information:

1. Click **Modem** from the main menu.
2. Click **Upstream** from the left side menu. Field descriptions are listed below the following screen example.



Label	Description
US-1 to US-4	Numbers the upstream channels.
Channel Type	Displays the channel type.
Channel ID	Displays the current cable modem upstream channel ID.
Frequency (Hz)	Displays the current cable modem upstream frequency in hertz.
Ranging Status	Displays the upstream ranging status.

Label	Description
Modulation	Displays the current cable modem upstream modulation type (QPSK/ QAM8 /QAM16/ QAM32/ QAM64/ QAM128/ QAM256).
Symbol Rate (Ksym/sec)	Displays the symbol rate.
Upstream Mini-Slot Size	Displays the current cable modem upstream mini-slot size in Timebase Ticks of 6.25.
Power Level (dBmV)	Displays the current cable modem upstream transmit power in decibel millivolts.
T-1	Indicates a valid UCD was not received.
T-2	Indicates a ranging maintenance broadcast was not received.
T-3	Displays range response (RNG-RSP) time expiration.
T-4	Displays range (RNG) time expiration. Double-digit T3 and T4 values could indicate a bonding, provisioning, or other such issue that results in a continual reboot.

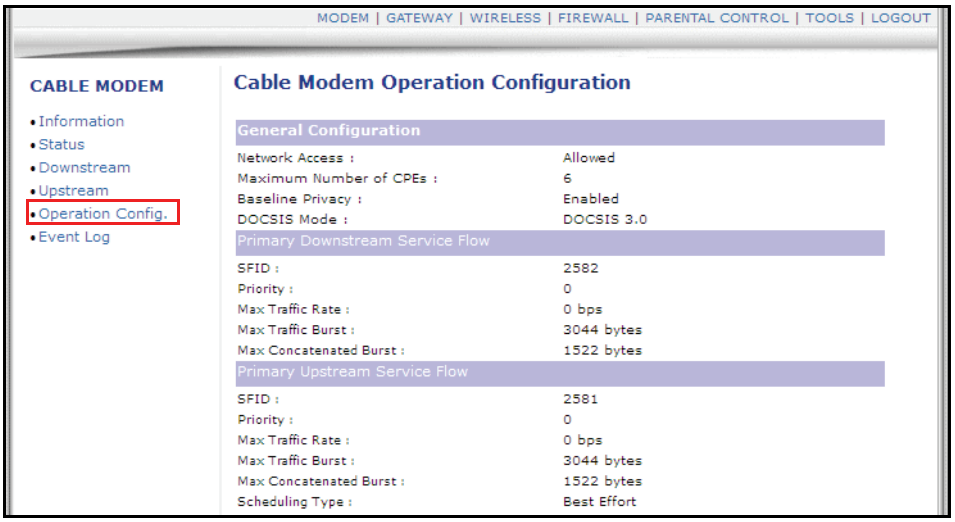
4.5 Using the Operation Config Option

The **Operation Config** screen displays general information on the device's active operational capabilities.

Steps

To view operation configuration information:

1. Click **Modem** from the main menu.
2. Click **Operation Config** from the left side menu. Field descriptions are listed below the following screen example.



Label	Description
General Configuration	
Network Access	Displays the status of the cable modem. ♦ Denied – Connectivity is not established. ♦ Allowed – Connectivity is established to the Internet.
Maximum Number of CPEs	Displays the maximum number of Ethernet devices that can be connected (LAN side) to access the network at the same time.
Baseline Privacy	Displays highlighted device configurations, such as PHS Enabled.
DOCSIS Mode	Displays the DOCSIS version of the device.
Primary Downstream Service Flow	
SFID	Displays the frequency ID of the downstream service flow.
Priority	Displays the priority level of the downstream service flow.
Max Traffic Rate	Displays the max data rate as enabled by the service provider.
Max Traffic Burst	Displays the max data rate as enabled by the service provider for downstream data bursts.
Max Concatenated Burst	Displays the max data rate per downstream burst.
Primary Upstream Service Flow	
SFID	Displays the frequency ID of the upstream service flow.
Priority	Displays the priority level of the upstream service flow.
Max Traffic Rate	Displays the max data rate as enabled by the service provider.
Max Traffic Burst	Displays the max data rate as enabled by the service provider for upstream data bursts.
Max Concatenated Burst	Displays the max data rate per upstream burst.
Scheduling Type	Displays the data scheduling type.

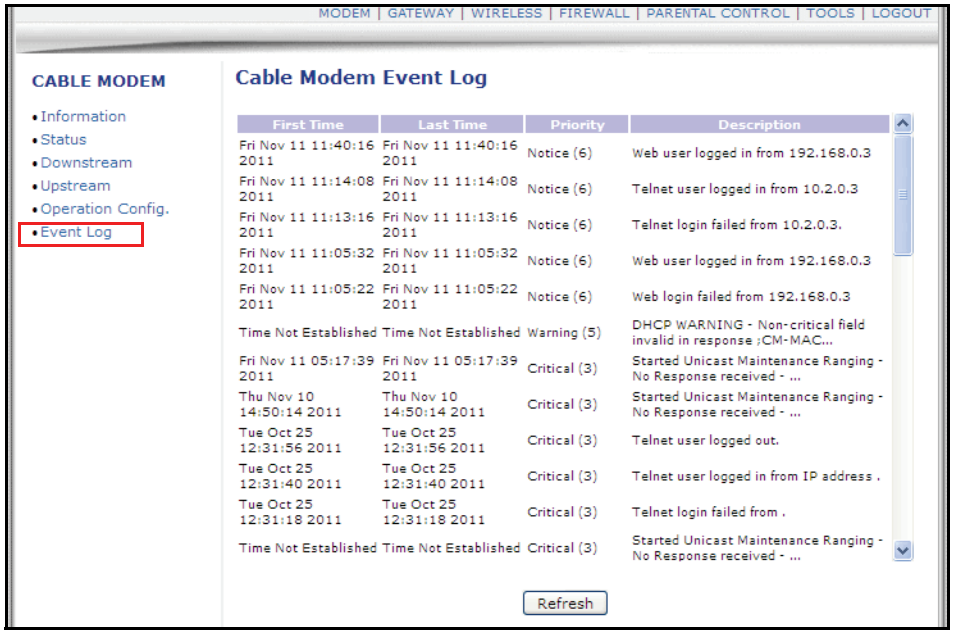
4.6 Using the Event Log Option

The **Event Log** screen displays log information that may be useful to diagnose operational issues with the device.

Steps

To view event log information:

1. Click **Modem** from the main menu.
2. Click **Event Log** from the left side menu. Field descriptions are listed below the screen example.



Label	Description
First Time	Displays the time the event started.
Last Time	Displays the last time the event was last recorded.
Priority	Displays the event log severity.
Description	Displays a detailed description of the event log.
Refresh	Updates the event log record to its most current state when you click Refresh.

5 Understanding the Gateway Menu

The Gateway functions provide the majority of configuration for the device including WAN IP addresses, LAN IP addresses, and DHCP. Advanced settings like DMZ, MAC filtering, and port forwarding are provided.

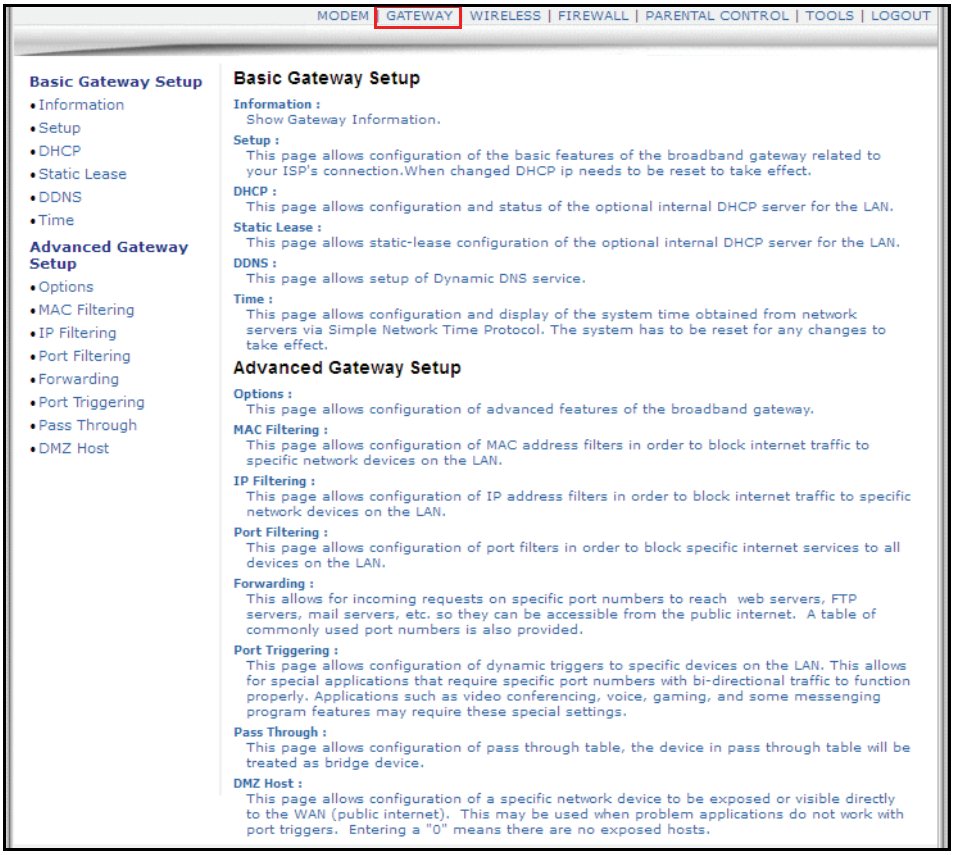
Topics

See the following topics:

Steps

To access the gateway menu:

1. Access the Web interface. Refer to Accessing the Web Interface on page 17.
2. Click **Gateway** from the main menu.



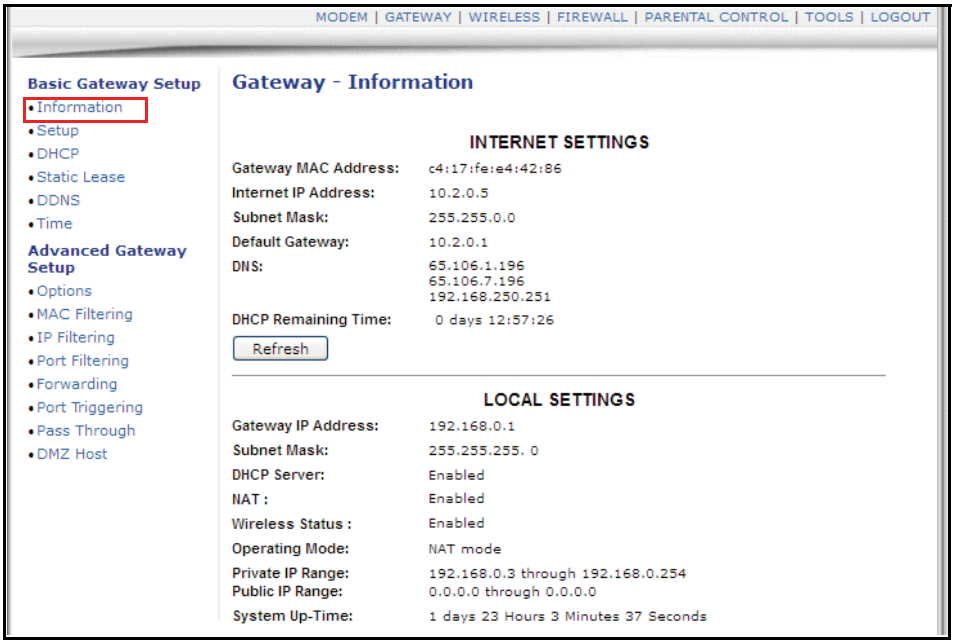
5.1 Using the Information Option

The **Information** option allows you to view basic information for the device.

Steps

To view gateway information:

1. Click **Gateway** from the main menu.
2. Click **Information** from the left side menu. Field descriptions are listed below the screen example.



Label	Description
Internet Settings	
Gateway MAC Address	Displays the Media Access Control (MAC) address of the residential gateway.
Internet IP Address	Displays the Internet IP address obtained from the service provider.
Subnet Mask	Displays the subnet mask of the Internet IP address.
Default Gateway	Displays the default gateway IP address.
DNS	Displays the DNS server IP address.
DHCP Remaining Time	Displays the time remaining on the DHCP lease before it expires.
Refresh	Updates the information to its most current state when you click Refresh.
Local Settings	
Gateway IP Address	Displays the local IP address of the LAN interface.
Subnet Mask	Displays the subnet mask value.
DHCP Server	Displays the status of the DHCP sever feature (Enabled/Disabled).
NAT	Displays the status of the NAT feature (Enabled/Disabled).
Wireless Status	Displays the status of the wireless feature (Enabled/Disabled).
Operating Mode	Displays which mode the router is in (Bridge, Router, Gateway). **Note**: Firewall menu options are not available when the device is in Bridge mode.

Label	Description
Private IP Range	Displays the private IP address assigned to DHCP client.
Public IP Range	Displays the Public IP DHCP Server Range.
System Up-Time	Displays the accumulated time since the last power cycle.

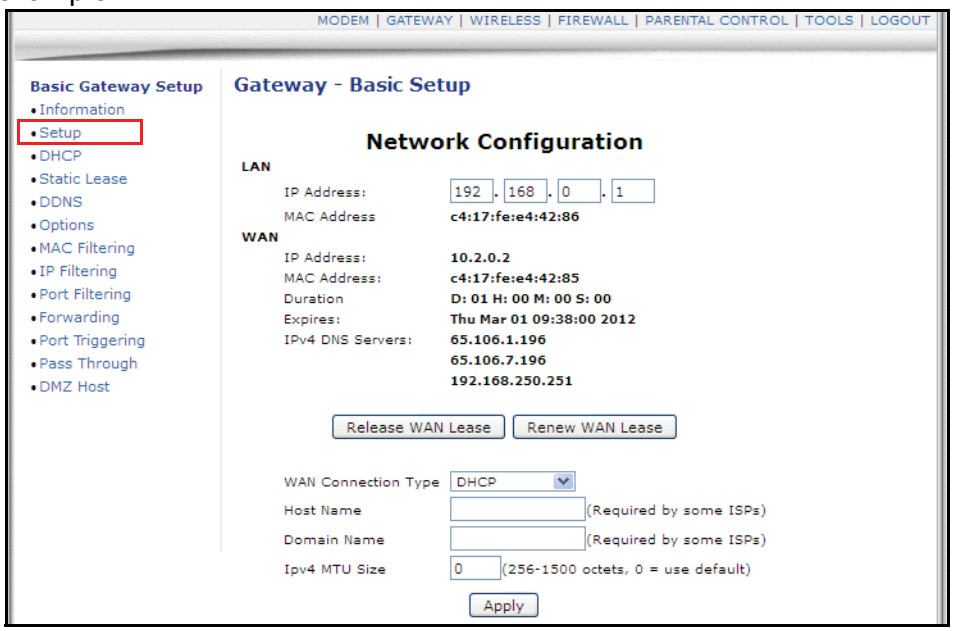
5.2 Using the Setup Option

The **Setup** option allows you to make basic configurations to the device.

Steps

To configure gateway settings:

1. Click **Gateway** from the main menu.
2. Click **Setup** from the left side menu. Field descriptions are listed below the screen example.

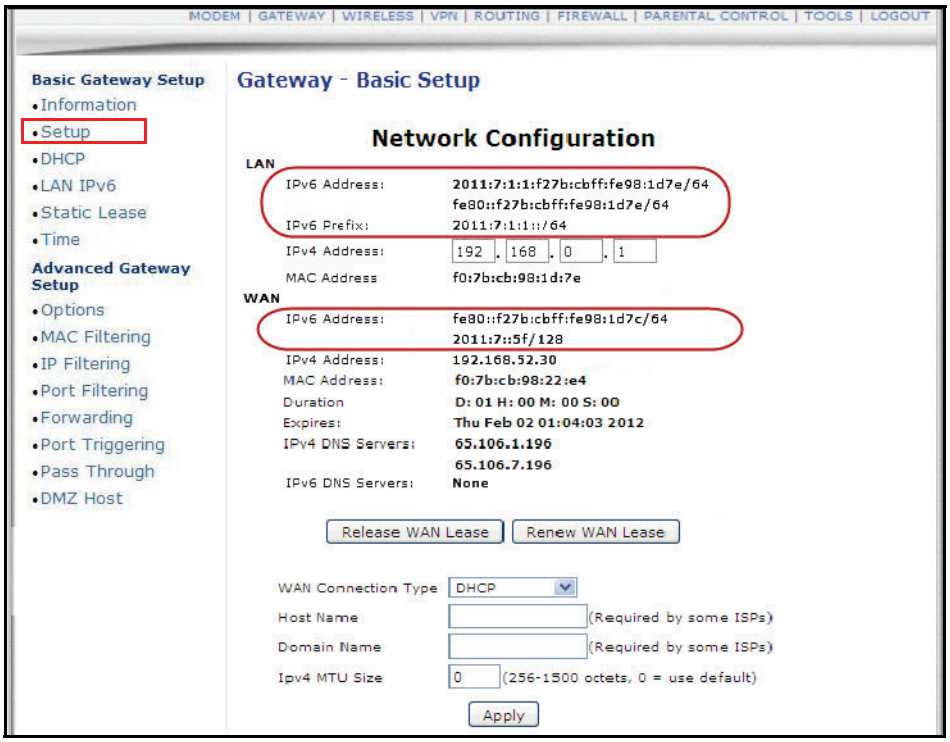


Label	Description
LAN	
IP Address	Defines the local IP address, which is the default gateway address for all wired LAN hosts that connect to the DDW3611.
MAC Address	Displays the LAN interface's hardware address.
WAN	
IP Address	Displays the current WAN public IP address obtained from the service provider.
MAC Address	Displays the WAN interface's hardware address.

Label	Description
Duration	Displays the accumulated time since successfully acquiring a WAN public IP address.
Expires	Displays the remaining time before the WAN IP address expires, if applicable.
IPv4 DNS Servers	Lists the DNS servers available on the network.
Release WAN Lease	Releases the WAN public IP address when clicked.
Renew WAN Lease	Renews the WAN IP address when clicked.
WAN Connection Type	Selects the WAN connection type. For each type, different data entry is required, as explained below: ♦ DHCP: The WAN interface is set to a DHCP client, and the IP address is assigned by the service provider's DHCP server. ♦ Static IP: For Static IP, you must manually enter the IP address for the WAN interface. ♦ PPTP (DHCP): For Point to Point Tunneling Protocol (PPTP), you must enter a username, password, and the PPTP server's IP address.
Host Name	Defines the host name for the router. This may be required by some service providers.
Domain Name	Defines the domain for the router. This may be required by some service providers.
IPv4 MTU Size	Defines the maximum transmission unit (MTU) size. MTU defines the largest size of the packet or frame that the device can transfer (256-1500). If this is not given by your service provider, use 0 for the default.
Apply	Saves all changes made in this screen when clicked.

5.2.1 Viewing IPv6 Addresses in the Gateway Setup Option

Additional IP addresses are needed to support the increase in Internet activity. Internet Protocol version 6 (IPv6) addressing is supported by the DDW3611 and displayed when the CMTS uses IPv6. The screen shot below displays an IPv6 address configuration in the Gateway Basic Setup option.



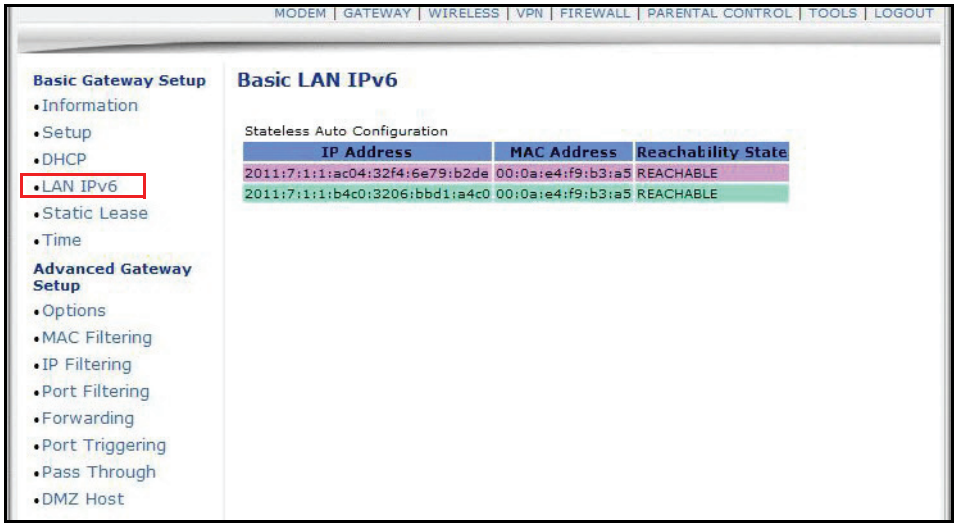
5.2.2 Using the LAN IPv6 Option

When the CMTS supports IPv6 address configuration, the LAN IPv6 option is available. The LAN IPv6 screen displays the assigned IP addresses which uses the Stateless Auto Configuration feature. Stateless Auto Configuration allows devices attached to an IPv6 network to connect to the Internet without requiring DHCP support.

Steps

To view assigned IPv6 addresses:

1. Click **Gateway** from the main menu.
2. Click **LAN IPv6** from the left side menu. Field descriptions are listed below the screen example.



Label	Description
IP Address	Displays the IPv6 address of the connected device.
MAC Address	Displays the MAC address of the connected device.
Reachability State	Displays the status of the neighboring device. Reachable indicates the device can be contacted and configuration information can be obtained from the device.

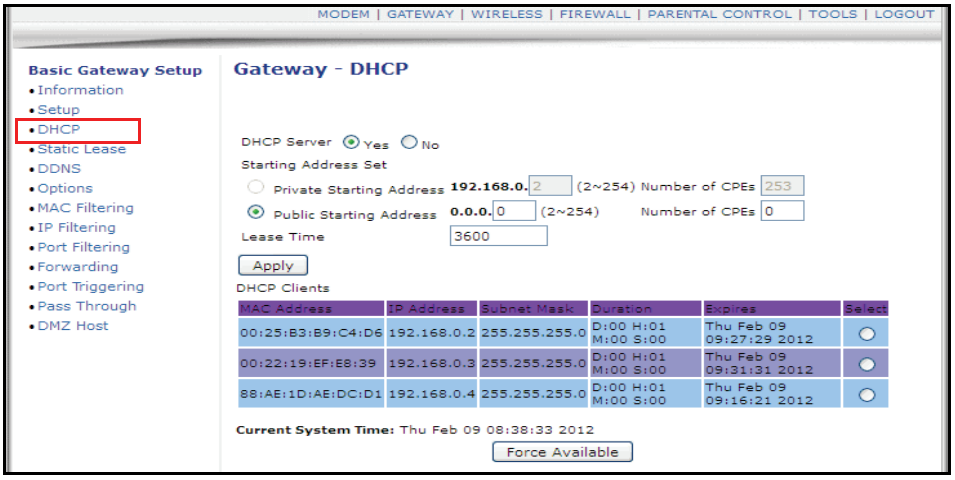
5.3 Using the DHCP Option

The dynamic host configuration protocol (**DHCP)** option allows you to configure DHCP-specific behavior on the device.

Steps

To configure DHCP settings:

1. Click **Gateway** from the main menu.
2. Click **DHCP** from the left side menu. Field descriptions are listed below the screen example.



Label	Description
DHCP Server	Enables (Yes) or disables (No) DHCP on the device. If No is selected, all the static DHCP rules in this screen are ignored.
Starting Address Set	
Private Starting Address	Defines the starting address for the pool of private IP addresses that can be used by connecting clients. Private addresses are translated to public IPs to be used on the network.
Public Starting Address	Defines the starting public IP address. Public addresses can be recognized on the network.
Number of CPEs	Defines the maximum number of customer premises equipment (CPE) that can connect to the network through the DDW3611.
Lease Time	Defines the DHCP lease time duration in minutes between 1 and 71582788. A DHCP user's PC gets an IP address with a lease time. When the lease time expires, the PC must connect to the DHCP server and be issued a new unused IP address. **Note:** The default DHCP lease time is 3600 seconds and should be changed to **86400** seconds (24 hours). This helps resolve connectivity issues with some iMAC and Windows 7 devices that turn off the network interface when they go into standby mode. This results in slow Web browsing until the device gets a new IP address via DHCP.

Label	Description
Apply	Applies and saves all changes when clicked.
DHCP Clients	Lists all DHCP clients currently connected to the device, either via an Ethernet link, or via a wireless connection. Each client is listed with the following information: ♦ MAC Address / IP Address / Subnet Mask ♦ Duration – Displays the accumulated time since the client acquired the IP address. ♦ Expires – Displays the time until the IP expires and must be recycled. If the IP address is reserved to a certain host, it shows STATIC IP ADDRESS. ♦ Select – Reserves the current private IP address to be assigned to this host statically when selected.
Force Available	Activates a selected rule in the DHCP Clients list and assigns IP addresses. Note: The Select button must be activated in the DHCP list.

5.4 Using the DHCP Static Lease Option

You can use the **Static Lease** option to assign IP addresses to clients on your network that do not change. A static lease ensures a specific device always gets the same IP address, especially if devices are powered on and off or disconnected and reconnected. This may be useful in a variety of networking scenarios where you need more control over the network and the clients that connect to it. Examples in which you may need to use a static lease include:

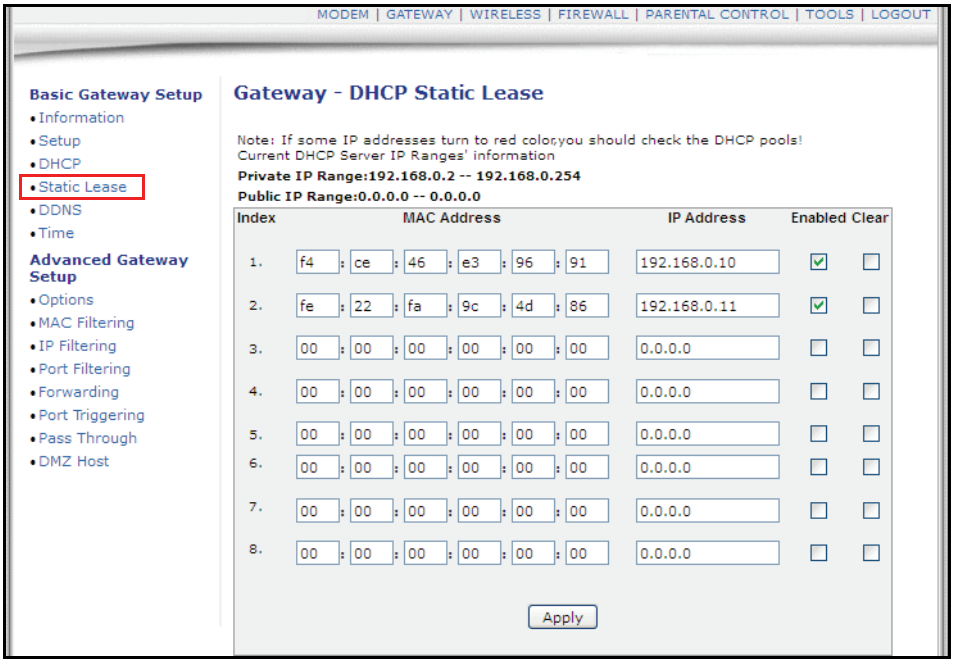
- Using the IP Filtering Option on page 44
- Using the Port Filtering Option on page 45
- Using the DMZ Host Option on page 53

Steps

To assign static IP addresses:

1. Click **Gateway** from the main menu.
2. Click **Static Lease** from the left side menu. Field descriptions are listed below the screen example.

   Note: The following example shows the DHCP Static Lease option set up for a dual Xbox configuration.



Label	Description
Index	Provides an index number for each client that connects to your network.
MAC Address	Defines the MAC address of the client to which you want to assign a static IP address.
IP Address	Defines an IP address to the specific client/host.
Enabled	Activates this rule when Enable is checked.
Clear	Deletes the rule when Clear is checked.
Apply	Saves all screen changes when clicked.

5.5 Using the DDNS Option

The dynamic domain name system (DDNS) allows a changing IP address to be assigned to a constant pre-defined host name. This allows the host to be contacted by other hosts on the Internet even if its IP address changes.

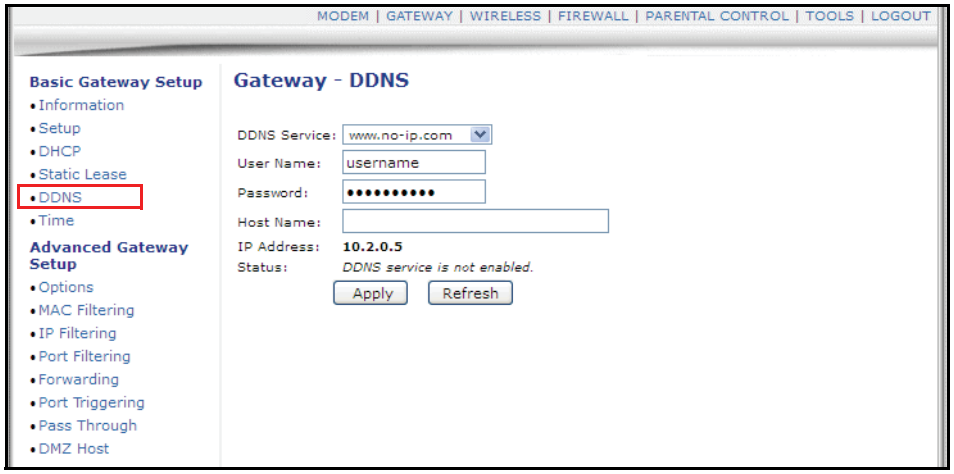
The DDNS service for the DDW3611 is provided through a third-party and can be purchased from Dynamic Network Services Inc. at www.dynDNS.com or No-IP at www.no-ip.com.

Steps

To use the DDNS option:

3. Click **Gateway** from the main menu.
4. Click **DDNS** from the left side menu. Field descriptions are listed below the screen

example.



Label	Description
DDNS Service	Enables or disables the DDNS service. When enabled, this service is available from www.dynDNS.org or www.no-ip.com.
User Name	Defines the user name for the DDNS account.
Password	Defines the password for the DDNS account.
Host Name	Defines the host name for the DDNS account.
IP Address	Displays the IP address for the DDNS account.
Status	Displays if the DDNS service is enabled or disabled.
Apply	Saves all screen changes when clicked.
Refresh	Renews the screen with the latest information.

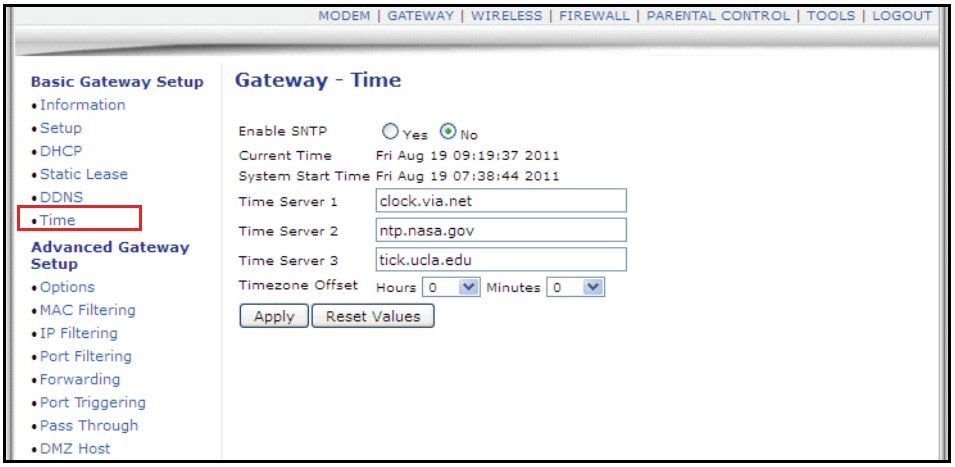
5.6 Using the Time Option

The **Time** option allows you to configure the system time obtained from network servers via Simple Network Time Protocol (SNTP).SNTP is a protocol for synchronizing the clocks of computing devices over networks. The device must be reset for changes to take effect.

Steps

To configure system time:

1. Click **Gateway** from the main menu.
2. Click **Time** from the left side menu. Field descriptions are listed below the screen example.



Label	Description
Enable SNTP	Enables (Yes) or disables (No) the SNTP feature.
Current Time	Displays the current system time.
System Start Time	Displays the accumulated time since the system was started.
Time Server 1	Defines the IP address or Domain name of the time server. Use the one provided or enter an alternative choice.
Time Server 2	Defines the IP address or Domain name of the time server. Use the one provided or enter an alternative choice.
Time Server 3	Defines the IP address or Domain name of the time server. Use the one provided or enter an alternative choice.
Time Zone Offset	Defines the time zone offset in hours and minutes from Greenwich MEan Time. For example: 8 hours means GMT +8, -1 hour means GMT -1.
Apply	Saves all screen changes when clicked.
Reset Values	Resets the screen to factory defaults when clicked.

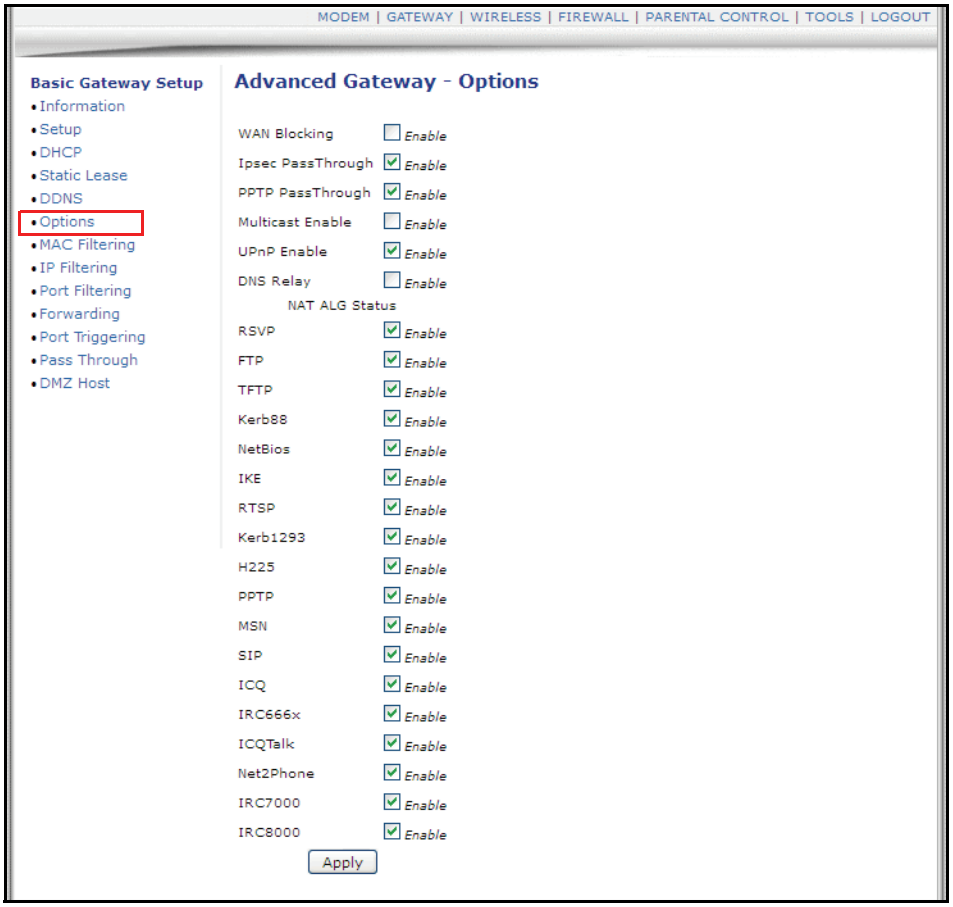
5.7 Using the Advanced Gateway Options

The **Options** selection allows you to define what networking protocols are enabled or disabled on the device. The network address translation application-level gateway (NAT ALG) settings provide additional security beyond the firewall.

Steps

To enable or disable network protocols:

1. Click **Gateway** from the main menu.
2. Click **Options** from the left side menu. Field descriptions are listed below the screen example.



Label	Description
WAN Blocking	Blocks connection requests initialized from Internet users when enabled. WAN Blocking must be disabled to be able to PING the WAN gateway IP.
Ipsec PassThrough	Forces the router to redirect the IPSec request to the local host when enabled. NAT fails this attempt if Internet users initialize an IPSec VPN request to a host located behind the router.
PPTP PassThrough	Forces the router to redirect the PPTP request to the local host when enabled. Nat fails this attempt if Internet users initialize a PPTP VPN request to a host located behind the router.
Multicast Enable	Optimizes the bandwidth utilization compared with unicast (especially video streaming applications).
UPnP Enable	Activates Universal Plug and Play (UPnP) when enabled. A UPnP device can dynamically join a network, obtain an IP address, convey its capabilities, and learn about other devices on the network. In turn, a device can leave a network smoothly and automatically when it is no longer in use. Gaming consoles and Web cameras are examples of devices that can use UPnP.

Label	Description
DNS Relay	Allows the cable modem to act as the “relay” device. Each PC that wants to access a URL does not have to send a DNS request to a DNS server on the Internet. DNS is used to resolve a URL (Web site name) to an IP address. DNS Relay is typically used for commercial applications where each device/PC connected to the cable modem uses the DNS Relay address rather than going to a public DNS server hosted by an ISP to look-up a URL.
NAT ALG Status – Filters to allow (enable) or disallow (disable) protocols to pass through the DDW3611 to connected devices (computers, game consoles, and so on).	
RSVP	Enables or disables resource reservation protocol (RSVP). RSVP defines how applications reserve resources and how they free the reserved resources once they are no longer needed.
FTP	Enables or disables the file transfer protocol (FTP) used to transfer files from one host to another.
TFTP	Enables or disables the trivial file transfer protocol (TFTP) – a simpler protocol generally used for automated file transfers.
Kerb88	Enables or disables the Kerberos network authentication protocol which allow nodes to communicate over a non-secure network using “tickets” on port 88 to prove their identity to one another.
NetBios	Enables or disables the network basic input/output system (NetBIOS) services related to the OSI session layer. NetBIOS allows applications on separate computers to communicate over a LAN.
IKE	Enables or disables the network key exchange (IKE) protocol used to set up a security association (SA) in the IPsec protocol suite.
RTSP	Enables or disables the real time streaming protocol (RTSP) network control protocol used to establish and control media sessions between end points.
Kerb1293	Enables or disables the Kerberos network authentication protocol which allow nodes to communicate over a non-secure network using “tickets” on port 1293.
H225	Enables or disables the H.225 protocol used to define messages and procedures for call signalling, media packetization, and registration, admission, and status (RAS) functions.
PPTP	Enables or disables the point-to-point tunneling protocol (PPTP) used to implement a virtual private network.
MSN	Enables or disables the Microsoft network protocol used for instant messaging.

Label	Description
SIP	Enables or disables the session initiation protocol application layer gateway (SIP ALG). SIP ALG inspects protocol packets and formats SIP message headers and SDP body to ensure proper signaling. **Note:** Some hosted VoIP services prefer this function to be performed by their own session border controller (SBC) and require the SIP ALG to be disabled. Some IP-PBXs may require SIP ALG enabled.
ICQ	Enables or disables the ICQ instant messaging program.
IRC666x	Enables or disables the Internet relay chat (IRC) protocol used for text messaging.
ICQTalk	Enables or disables the ICQTalk instant messaging program.
Net2Phone	Enables or disables Net2Phone SIP VoIP.
IRC7000	Enable or disables the Internet relay chat protocol on TCP port TCP 7000 used for text messaging and group forums.
IRC8000	Enable or disables the Internet relay chat protocol on UDP port 8000 used for text messaging and group forums.
Apply	Saves all screen changes when clicked.

5.8 Using the MAC Filtering Option

MAC Filtering allows you to filter MAC addresses to block Internet traffic from specific network devices on the LAN. MAC filtering establishes a list and any host on this list is not able to access the network through the DDW3611.

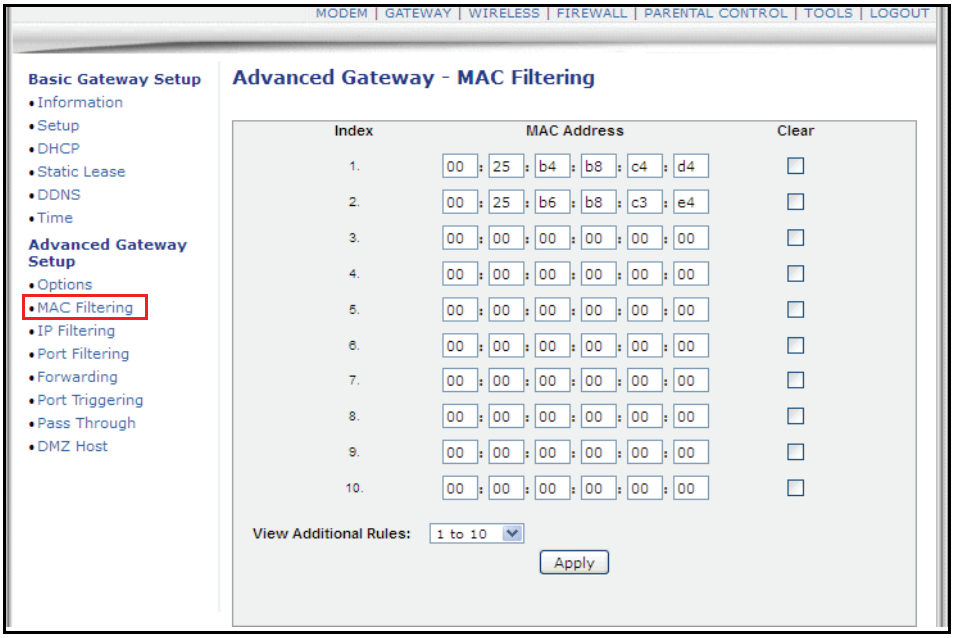
Steps

To filter MAC addresses:

1. Go to **Tools** > **Client List**. Your PC and other devices are listed. Note the MAC address of the devices you want to deny Internet access. For more information, refer to Using the Client List Option on page 83.

   Note – Be sure all devices to which you want to deny Internet access are connected to the DDW3611 network.

2. Click **Gateway** from the main menu.
3. Click **MAC Filtering** from the left side menu. Field descriptions are listed below the screen example.



Label	Description
Index	Assigns an index number to the rule.
MAC Address	Defines the MAC address to block.
Clear	Deletes the filtering rule when the Apply button is clicked and the Clear box is checked.
View Additional Rules:	Displays rules 11-20 when selected from the drop-down list, if they exist. A total of twenty rules are supported.
Apply	Saves all screen changes when clicked.

5.9 Using the IP Filtering Option

IP Filtering allows you to filter IP addresses and block Internet traffic to specific network devices on the LAN. Any host on this list is not accessible to Internet traffic.

For more information, refer to Using the DHCP Static Lease Option on page 37. A static lease ensures that the device always gets the same IP address. That way, if filtered, it gets filtered continuously. Otherwise, the IP address would change for the device and the filtering rule would no longer work.

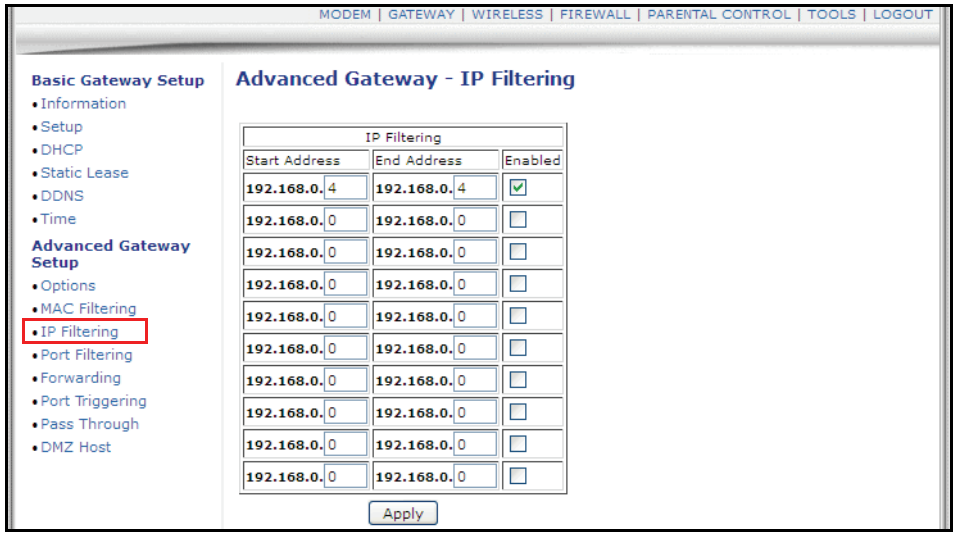
Note

You may also filter by MAC address which does not require setting a static lease. Refer to Using the MAC Filtering Option on page 43.

Steps

To set up IP filtering.

1. Make sure a PC is connected to the cable modem and both devices are powered on and functioning.
2. Go to **Tools** > **Client List** in the Web user interface. Refer to Accessing the Web Interface on page 17. Your PC and other devices are listed.
3. Note the MAC address and IP address of the devices to which you want to deny Internet access. For more information, refer to Using the Client List Option on page 83.
4. Click **Gateway** from the main menu.
5. Click **IP Filtering** from the left side menu.
6. Enter the MAC address and IP address of devices to which you want to deny Internet access.
7. Click **Apply**. Field descriptions are listed below the screen example.



Label	Description
Start Address	Defines the starting IP address to filter.
End Address	Defines the ending IP address to filter.
Enabled	Activates the rule when enabled is checked.
Apply	Saves all screen changes when clicked.

5.10 Using the Port Filtering Option

Port Filtering allows you to configure port filters to block to all devices on the LAN Internet services that use specific ports.

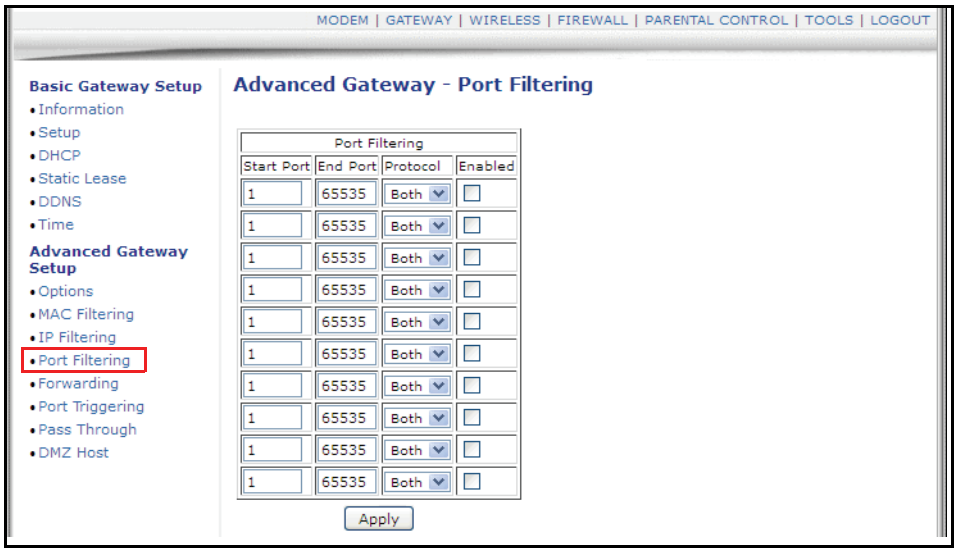
For example, to prevent all Telnet access into and across your LAN, you would enter the **Start** and **End** ports to be 23, select Both for **Protocol**, and click the **Enabled** selection box.

Be careful using port filtering by port range as you may accidentally prevent traffic that should pass through your network (for example, http or email). To see what applications use each port, refer to Using the Forwarding Option on page 47 and click the **Port Map** button.

Steps

To configure port filters:

1. Click **Gateway** from the main menu.
2. Click **Port Filtering** from the left side menu. Field descriptions are listed below the screen example.



Label	Description
Start Port	Defines the starting port number
End Port	Defines the ending port number.
Protocol	Selects the protocol type. Options are UDP, TCP, or BOTH.
Enabled	Activates the rule and filters out all traffic on the specified ports.
Apply	Saves all screen changes when clicked.

5.11 Using the Forwarding Option

Port forwarding allows you to tell the cable modem which computer on the local area network to send the data. You can set up applications/services to listen on one internal port. External Internet users who want to access that application address it using an external port, such as an Audio server.

Use port forwarding to resolve issues when:

- Data is sent from a local host to the Internet, but your local host does not receive the expected data
- An application or service running on your local network (on local host) cannot be accessed from the Internet directly (for example, a request to a local audio server).

Some examples of when you might need forwarding:

- Xbox/PlayStation – Games/applications.
- Home Security Systems – Security systems that use the Internet.
- Audio Servers/VoIP – Audio and VoIP applications and services.

Port forwarding requires the following information:

- **IP address** of each local host system (for example, Xbox) for port forwarding rule you need to set up. See Using the Client List Option on page 83 to obtain the MAC and IP address of the internal host for which you are setting up a forwarding rule.
- **Port numbers** to which the local host's application listens to detect incoming requests/data. For example, a game or other service. Port numbers are usually available in the documentation associated with the application, or refer to http://portforward.com.

Note

If your host system/application does **not** have communication issues with the Internet, you do not need port forwarding

Topics

See the following topics:

- Before Setting Up Forwarding Rules on page 47
- Assigning a Static Lease on page 48
- Setting Up Forwarding for an Xbox (Example): on page 48
- Viewing Port Maps on page 50

5.11.1 Before Setting Up Forwarding Rules

Before you set up forwarding rules, we recommend you enable UPnP to see if this resolves your communication issue. See Using the Advanced Gateway Options.

Steps

To enable UPnP:

3. From the Web UI, click **Gateway** from the main menu, and then **Options** from the left side menu.
4. Check the **UPnP Enable** box on the **Advanced Gateway - Options** page.
5. Test your local host/application, for example an Xbox. If it is working properly, you do not need to set up forwarding rules. If not, continue to Assigning a Static Lease.

5.11.2 Assigning a Static Lease

If enabling UPnP did not solve your communication issue, we recommend setting up forwarding rules.

First, we suggest assigning a static IP. By assigning a static IP lease to the client/host to which you are setting up forwarding, (see Using the DHCP Static Lease Option on page 37), the IP will not change and disrupt your forwarding rules. For example, if you are hosting a Web server in your internal network, and you want to set up a forwarding rule for it, first assign a static IP lease to that system to stop the IP from renewing and disrupting the forwarding rule.

5.11.3 Setting Up Forwarding for an Xbox (Example):

This example shows how to setup a single Xbox running Modern Warfare 2. Since multiple ports are used for the Xbox and the Modern Warfare 2 game, a separate forwarding rule is set up for each port. Multiple ports and forwarding rules may not be required for other applications.

Steps

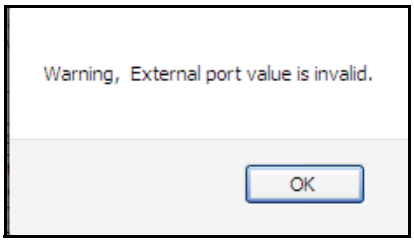
To set up forwarding for an Xbox:

1. Click **Gateway** from the main menu.
2. Click **Forwarding** from the left side menu. Field descriptions are listed below the screen example.
3. Enter the Xbox IP address in the **Local IP** field. Enter the same IP in 4 rows, one row for each port used by the Xbox.
4. Define the ports used by the Xbox in the **Internal Port** field. Internal Ports are the ports to which local servers listen.

   You need to create a forwarding rule for each port. A rule set up for port 53 works only for port 53, because a port can be used by only one program at a time.
5. Define the same ports used by the Xbox in the External Port Start and End fields. External Ports are the ports that the cable modem listens to from the WAN.
6. Check **Enabled** for each entry.

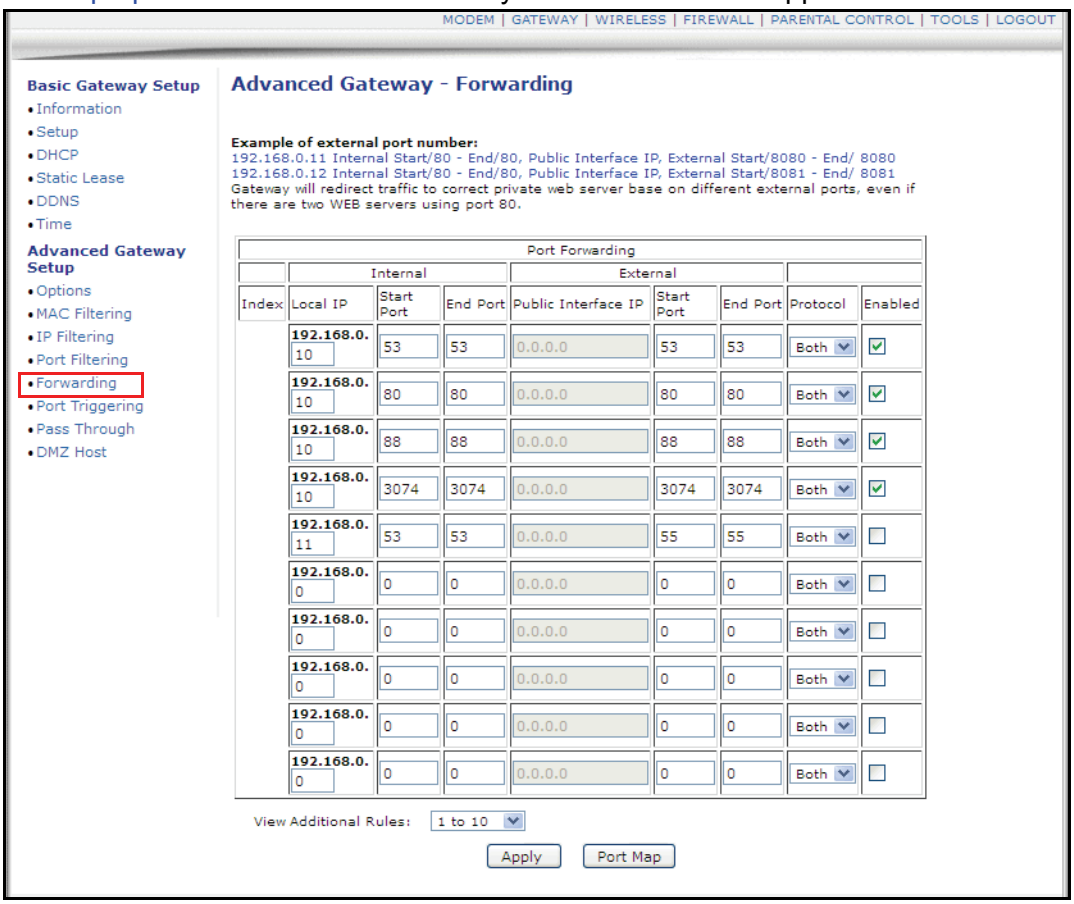
7. Click **Apply**.

   If a duplicate or overlapping port range is entered, you receive a warning and external ports are reset to 0:



Note – Duplicate entries imported to the forwarding table from older versions will be disabled.

For detailed information on port forwarding, including how to set it up for applications using specific network devices (for example, cable modems), refer to: http://portforward.com or consult your host device or application user manual.



Label	Description
Internal	
Index	Displays the Index number of the rule.

Local IP	Defines the last digits of the IP address of the local LAN device to which the forwarding rule applies,. For example, an Xbox or PC.
Start Port	Defines the starting port number listened to by the server host located in your LAN.
End Port	Defines the ending port number listened to by the server host located in your LAN.
External	
Public Interface IP	Designates another router on the network to forward data through. Normally, this field is not modified.
Start Port	Defines the port number to start the range of ports to publish to the Internet.
End Port	Defines the port number to end the range of ports published to Internet. Note: Be careful when assigning post ranges. Ports within a range are not usable by other applications that may require them. We recommend using the same port number as the start and end of each range.
Protocol	Selects the protocol type. Options are UDP, TCPIP, or Both.
Enabled	Enables this rule when checked.
View Additional Rules	Displays rules 11-20 when selected from the drop-down list, if they exist. A total of twenty rules are supported.
Apply	Saves all screen changes when clicked.
Port Map	Shows a list of common applications and their ports.

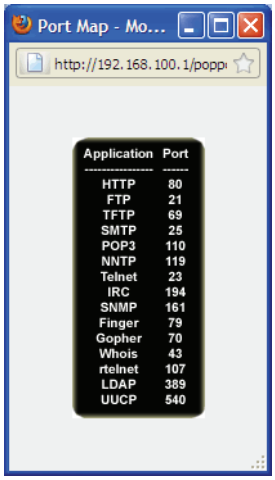
5.11.4 Viewing Port Maps

Port maps display a list of common applications and the port to which they are assigned. This option is available from the Forwarding screen.

Steps

To view assigned port maps:

1. On the Advanced Gateway – Forwarding screen, click **Port Map** at the bottom of the screen.
2. View the application names and pre-assigned port numbers.



3. Click to close the Port Map window.

5.12 Using the Port Triggering Option

Port Triggering assigns dynamic triggers to specific devices on the LAN. Special applications requiring specific port numbers with bi-directional traffic can then function properly. Applications such as video conferencing, gaming, and some messaging program features may require these special settings.

Some services use a dedicated range of ports on the client and server sides. With port forwarding, you define a rule to send a service to the IP address of a LAN side host. Port forwarding sends a service to a **single** LAN IP address.

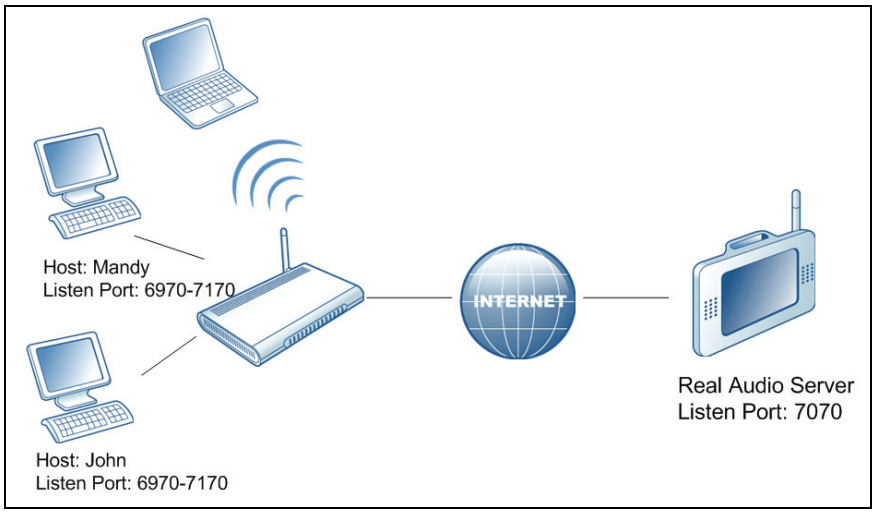
Port triggering defines two kinds of ports and the server returns responses to these ports:

- Trigger port – A service request with a specific destination port number sent from a LAN side host.
- Target Port – A port this specific application requires a LAN host to listen to.

For example:

1. John requests a file from the Real Audio server (port 7070). Port 7070 is a “trigger” port and causes the device to record John’s IP address. The DDW3611 associates John’s computer IP address with the “target” port range of 6970-7170.
2. The Real Audio server responds to a port number ranging between 6970-7170.
3. The DDW3611 forwards the traffic to John’s IP address.

4. Only John can connect to the Real Audio server until the connection is closed or times out.



Steps

To set up port triggering:

1. Click **Gateway** from the main menu.
2. Click **Port Triggering** from the left side menu. Fields are described following the screen example.

Label	Description
Trigger Range	Defines the trigger port or a range of ports that trigger the router to record the IP address of the LAN computer that sent the traffic to a server on the WAN.
Start Port	Defines a port number or the starting port number in a range of port numbers.
End Port	Defines a port number or the ending port number in a range of port numbers.
Target Range	Defines a target range port or a range of ports a server on the WAN uses when it responds to service requests. The router forwards the traffic with this port (or range of ports) to the client computer on the LAN that requested the service.
Start Port	Defines a port number or the starting port number in a range of port numbers.
End Port	Defines a port number or the ending port number in a range of port numbers.
Protocol	Defines the protocol type for this rule, UDP, TCP, or Both.
Enable	Activates this rule when checked.
Apply	Saves all screen changes when clicked.

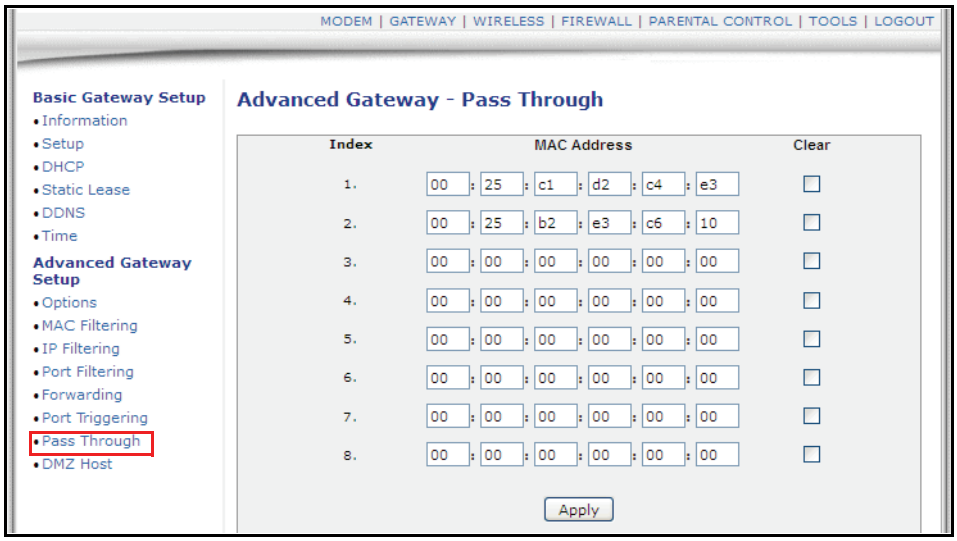
5.13 Using the Pass Through Option

The **Pass Through** option allows you to configure a pass through table. Devices in the pass through table are treated as bridge devices that store and forward data between LAN interconnections.

Steps

To set up a pass through table:

1. Click **Gateway** from the main menu.
2. Click **Pass Through** from the left side menu. Field descriptions are listed below the screen example.



Label	Description
Index	Defines the index number of the pass through rule.
MAC Address	Defines the input host's MAC address.
Clear	Deletes this rule when checked and the Apply button is clicked.
Apply	Saves all screen changes when clicked.

5.14 Using the DMZ Host Option

The **DMZ Host** option allows you to configure a host IP address to be exposed (visible) to the WAN (public Internet). This may be used when applications do not work with port triggers or other networking strategies.The following instructions are best practices when adding a device into a DMZ

Steps

To configure a DMZ host:

1. Connect a PC to an Ethernet port on the DDW3611. Make sure both devices are powered on and functioning.
2. Connect a Home Gateway (or other device you wish to be in the DMZ) to an Ethernet port on the DDW3611.
3. Log in to the DDW3611 Web user interface.
4. Go to **Tools** > **Client List**. Your PC and other devices are listed.
5. Note the MAC address and IP address of the Home Gateway, VoIP Phone, or other device to put in the DMZ. For more information, refer to Using the Client List Option on page 83.
6. Go to **Gateway** > **Static Lease**. Enter the MAC address and IP address of a Home Gateway (or other device you wish to be in the DMZ).
7. Click **Apply**. For more information, refer to Using the DHCP Static Lease Option on page 37. A static lease ensures that the device is assigned the same IP address so it is always available on the network, especially if devices are powered on/off or disconnected and reconnected.
8. Click **Gateway** from the main menu.
9. Click **DMZ Host** from the left side menu. Field descriptions are listed below the screen example.
10. Enter the IP address you just configured in the Static Lease section.
11. Test the device to ensure Internet access is available and the device is functional. For example, connect to the Internet from a PC connected to the Home Gateway, or make calls from a VoIP phone.

The following example shows the DMZ Host set up for a dual Xbox configuration.

Label	Description
DMZ Address	Defines the IP address of the host to be exposed.
Apply	Saves all screen changes when clicked.

6 Understanding the Wireless Menu

This Wireless menu provides settings to configure a wireless network.

Topics

See the following topics:

Steps

To access the wireless menu:

1. Access the Web interface. Refer to Accessing the Web Interface on page 17.
2. Click **Wireless** from the main menu.

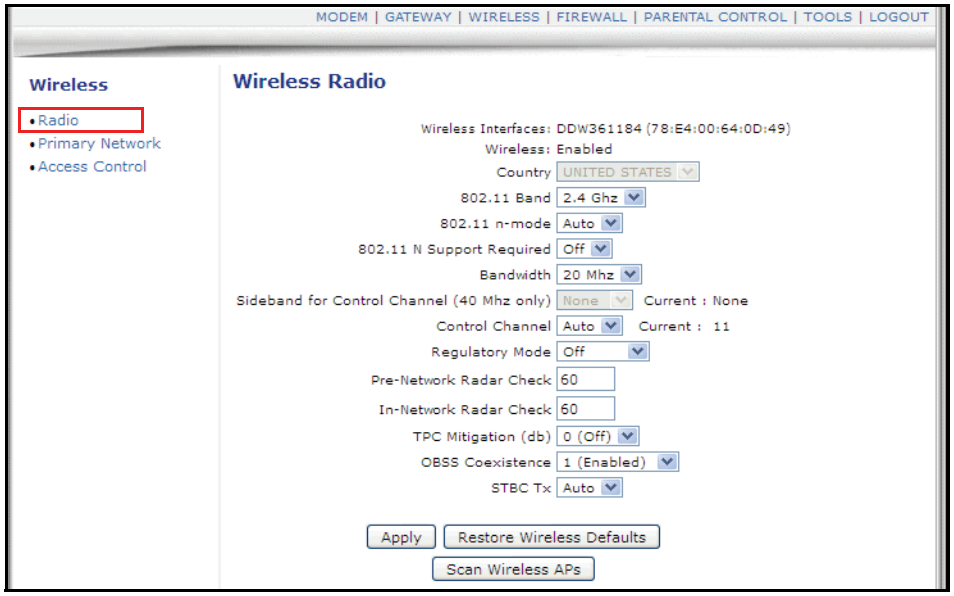
6.1 Using the Wireless Radio Option

The **Radio** option is used to configure the wireless radio, including the current country, channel number, and bandwidth control.

Steps

To configure wireless operations:

1. Click **Wireless** at the main menu.
2. Click **Radio** from the left side menu. Field descriptions are listed below the following screen example.



Label	Description
Wireless Interfaces	Displays the wireless name and MAC address.
Wireless	Displays the wireless radio's status, Enabled or Disabled.
Country	Defines the country where this device is used.
Output Power	Sets the percent of the Output Power for the radio.
802.11 Band	Defines the radio band as 2.4Ghz or 5 Ghz. **Note**: The distance coverage for 5Ghz is less than 2.4Ghz.
802.11 n-Mode	Sets the wireless networking standard. Select Auto to use 802.11 n mode when possible. This mode has a significant increase in the maximum raw OSI physical layer data rate from 54 Mbps to a maximum of 600 Mbps with the use of four spatial streams when at a channel width of 40 MHz. One spatial stream at 20MHz wide channel enables 72.2Mbps maximum data rate in 802.11n mode
802.11 N Support Required	Defines whether 802.11n support is required (on) or not (off). On forces the gateway to 802.11n mode and clients must support 802.11n.
Bandwidth	Sets the bandwidth to 20Mhz or 40Mhz. For 40 Mhz, set the sideband to lower or upper 20Mhz. 40 MHz channels double the channel width. This allows doubling the PHY data rate over a single 20 MHz channel.
Sideband for Control Channel (40 Mhz only)	Sets the sideband control to the lower or upper 20 MHz when the bandwidth is set to 40Mhz.
Control Channel	Selects a specific channel 1-11 to deploy the wireless network. This allows you to set the operating frequency/channel depending on your particular region. Channel selection can have an impact on wireless networking performance. For more information, refer to Selecting a Wireless Channel on page 69

Label	Description
Regulatory Mode	Defines whether Regulatory Mode is set to off, 802.11d, or 802.11h.
Pre-Network Radar Check	Defines the number of seconds to check for radar on a channel before establishing a network. Current specs specify 60 seconds. Range 0-99. Zero disables checking. Designed so APs avoid channels that contain radar systems. Used for 802.11h only.
In-Network Radar Check	Defines the number of seconds to check for radar when switching to a new channel after a network has been established. Current specs specify 60 seconds. Range: 10-99. Cannot be disabled. Designed so APs avoid channels that contain radar systems. Used for 802.11h only.
TPC Mitigation (dB)	Sets TPC Mitigation to 0 (off), 2,3, or 4.
OBSS Coexistence	Enables or disables overlapping BSS coexistence.
STBC Tx	Sets the space-time block codes (STBCs) for the transmitting antenna.
Apply	Saves all screen changes when clicked.
Restore Wireless Defaults	Restores the factory default settings for wireless configurations when clicked.
Scan Wireless APs	Scans for other wireless access points and displays channel, encryption, SSID, RSSI levels, and other information.

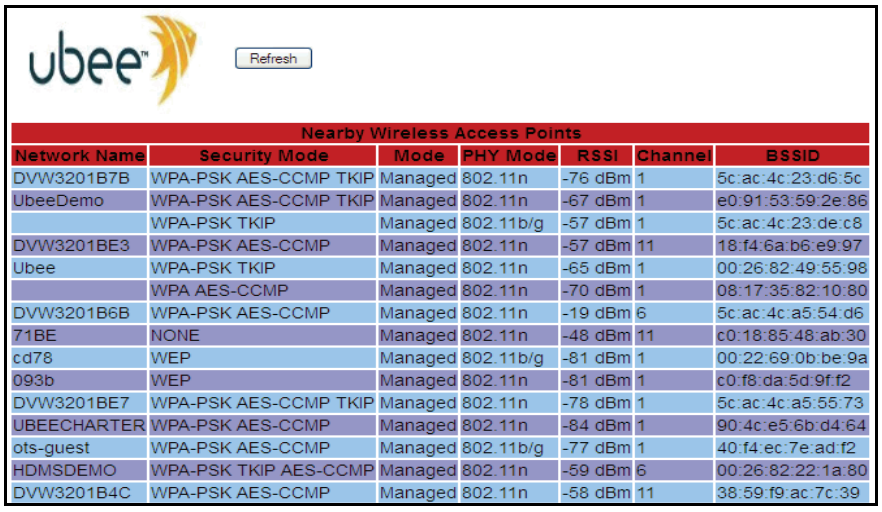
6.1.1 Scanning for Wireless Access Points (APs)

You can search for wireless access points and display the results in a new window.

Steps

To search for wireless access points:

1. Click **Scan Wireless APs** at the bottom of the Wireless Radio screen. Results are displayed in a new window.



Refresh

Nearby Wireless Access Points

Network Name	Security Mode	Mode	PHY Mode	RSSI	Channel	BSSID
DVW3201B7B	WPA-PSK AES-CCMP TKIP	Managed	802.11n	-76 dBm	1	5c:ac:4c:23:d6:5c
UbeeDemo	WPA-PSK AES-CCMP TKIP	Managed	802.11n	-67 dBm	1	e0:91:53:59:2e:86
	WPA-PSK TKIP	Managed	802.11b/g	-57 dBm	1	5c:ac:4c:23:de:c8
DVW3201BE3	WPA-PSK AES-CCMP	Managed	802.11n	-57 dBm	11	18:f4:6a:b6:e9:97
Ubee	WPA-PSK TKIP	Managed	802.11n	-65 dBm	1	00:26:82:49:55:98
	WPA AES-CCMP	Managed	802.11n	-70 dBm	1	08:17:35:82:10:80
DVW3201B6B	WPA-PSK AES-CCMP	Managed	802.11n	-19 dBm	6	5c:ac:4c:a5:54:d6
71BE	NONE	Managed	802.11n	-48 dBm	11	c0:18:85:48:ab:30
cd78	WEP	Managed	802.11b/g	-81 dBm	1	00:22:69:0b:be:9a
093b	WEP	Managed	802.11n	-81 dBm	1	c0:f8:da:5d:9f:f2
DVW3201BE7	WPA-PSK AES-CCMP TKIP	Managed	802.11n	-78 dBm	1	5c:ac:4c:a5:55:73
UBEECHARTER	WPA-PSK AES-CCMP	Managed	802.11n	-84 dBm	1	90:4c:e5:6b:d4:64
ots-guest	WPA-PSK AES-CCMP	Managed	802.11b/g	-77 dBm	1	40:f4:ec:7e:ad:f2
HDMSDEMO	WPA-PSK TKIP AES-CCMP	Managed	802.11n	-59 dBm	6	00:26:82:22:1a:80
DVW3201B4C	WPA-PSK AES-CCMP	Managed	802.11n	-58 dBm	11	38:59:f9:ac:7c:39

2. Click **Refresh** to update the results.

Label	Description
Network Name	Displays the name of the wireless network (SSID) broadcast by the access point.
Security Mode	Displays the encryption method used.
Mode	Displays the mode of the wireless access point: Possible modes are: ♦ **Master** – Communicates with associated wireless cards that are in managed mode. Appears as a normal access point with an SSID and channel. Network communications, such as authentication, conflict, and duplicate packets are managed by the wireless card. ♦ **Managed** – Communicates with an associated master, not directly with another managed AP. Wireless cards connect to the master network and change their channel to match. The master must accept the credentials of the managed network for it to be associated. ♦ **Ad-hoc** – Communicates directly with another wireless network. Network cards must be in range and use the same name and channel. ♦ **Monitor** – Communicates in observation mode and does not transmit. Can be used for troubleshooting wireless links or checking bandwidth usage in the area.
PHY Mode	Displays the physical transceivers (PHY) layer method used.
RSSI	Displays the received signal strength (RSSI) of the wireless access points in range of the device. Lower negative numbers (for example, -1 to -65) indicate the access point is closer. Greater negative numbers (for example, -66 to -95) indicate the access point is farther away.
Channel	Displays the channel on which the wireless cable modem is operating.
BSSID	Displays the MAC address for the nearby wireless access points.

6.2 Using the Primary Network Option

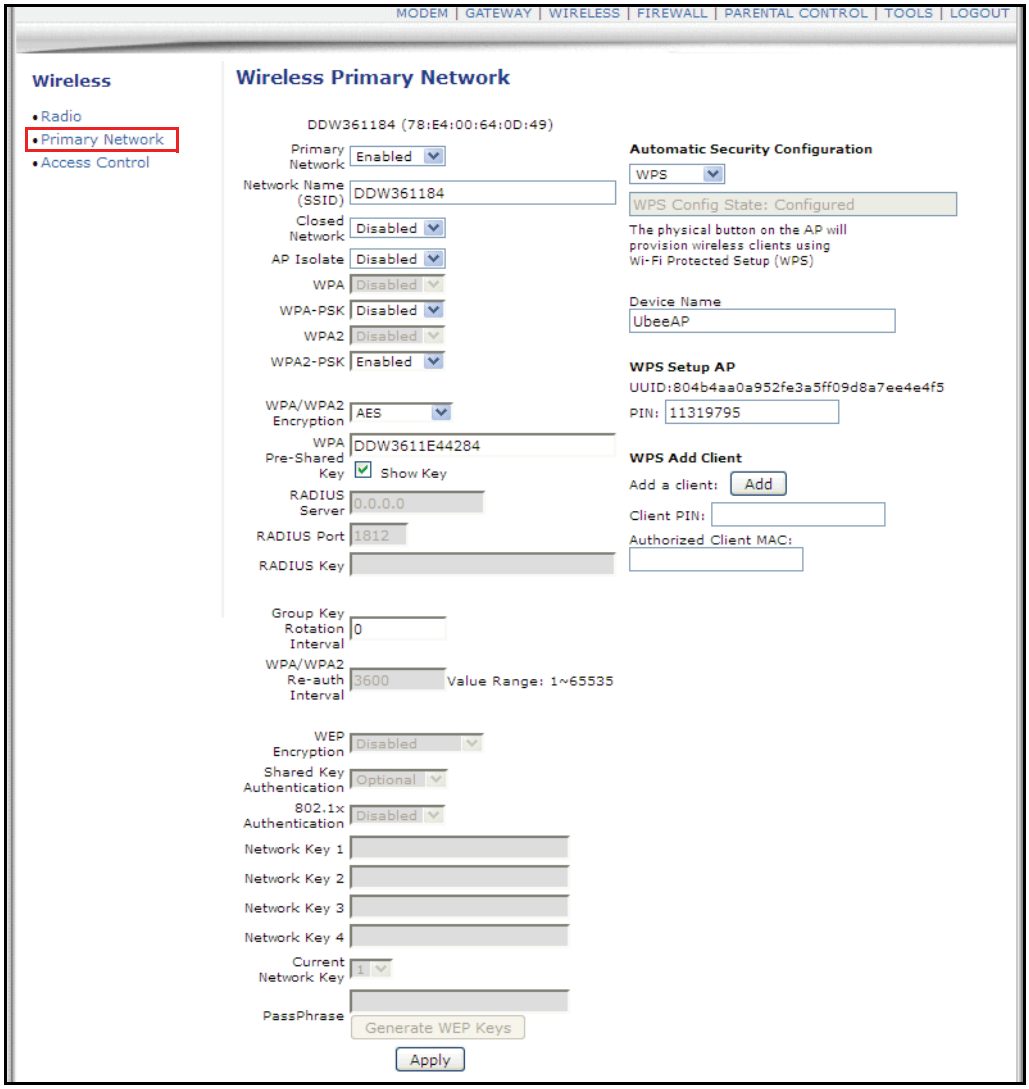
The **Primary Network** option allows you to configure a variety of wireless security settings.

Steps

To configure wireless security options:

1. Click **Wireless** from the main menu.
2. Click **Primary Network** from the left side menu. Field descriptions are listed below the screen example.

   Note: Wireless default values are discussed in Understanding Default Values and Logins on page 7.



Label	Description
Primary Network	Enables or disables the primary network.
Network Name	Defines the unique SSID of the cable modem or accept the default. Refer to Understanding Default Values and Logins on page 7 for more information on the SSID.
Closed Network	Hides the selected SSID when enabled so it is not visible to wireless clients unless manually set up on the client. If disabled, the SSID is visible. Refer to Enabling a Closed Network on page 64 to set up a closed network.
AP Isolate	Prevents wireless client stations from communicating with each other when enabled.
WPA	Enables or disables the Wi-Fi Protected Access (WPA) security protocol. WPA is a subset of the IEEE 802.11i standard. Key differences between WPA and WEP are user authentication and improved data encryption. Setting WPA alone with a pre-shared key requires a RADIUS or TACACS server for authentication. This method is mostly used in large enterprise implementations.
WPA-PSK	Enables or disables WPA Pre-Shared Key (WPA-PSK). If you do not have an external RADIUS server, use WPA-PSK, which requires a single (identical) password entered into wireless gateway and wireless client. As long as the passwords match, a client is granted access to the wireless LAN. This is the default residential subscriber setting and uses TKIP encryption.
WPA2	Enables or disables WPA2. This advanced protocol is certified through Wi-Fi Alliance's WPA2 program and implements the mandatory elements of 802.11i. In particular, it has an AES-based algorithm (CCMP) that is considered fully secure. Setting WPA2 alone with a pre-shared key requires a RADIUS or TACACS server for authentication. This method is mostly used in large enterprise implementations.
WPA2-PSK	Enables or disables WPA2-PSK. If you do not have an external RADIUS server, use WPA2-PSK, which requires a single (identical) password entered into wireless gateway and wireless client. As long as the passwords match, a client is granted access to the wireless LAN. This is the recommended residential subscriber option. It is more secure than WPA-PSK and uses AES encryption.
WPA/WPA2 Encryption	Sets WPA/WPA2 encryption to AES or TKIP+AES. The default is AES.
WPA Pre-Shared Key	Displays (checked) or hides (unchecked) the WPA key. The encryption mechanisms for WPA and WPA-PSK are the same, except that WPA-PSK uses a simple common password instead of user-specific credentials. Refer to Understanding LED Operations on page 8 for the default value of the shared key.
RADIUS Server	Defines the IP address of the RADIUS server, if used.

Label	Description
RADIUS Port	Defines a RADIUS port number when WPA or 802.1x network authentication is selected.
RADIUS Key	Defines the RADIUS Key when WPA or 802.1x network authentication is selected.
Group Key Rotation Interval	Allows the device to generate the best possible random group key and update all the key-management capable stations periodically.
WPA/WPA2 Re-auth Interval	Sends a new group key to all clients at the specified interval for a wireless router (if using WPA-PSK key management) or RADIUS server (if using WPA key management). The re-keying process is the WPA equivalent of automatically changing the WEP key for a wireless access point and all stations in the WLAN on a periodic basis. Setting the WPA Group Key Update Timer is also supported in WPA-PSK mode.
WEP Encryption	Enables or disables WEP encryption. If you do not have wireless clients that can use WPA or WPA2, you can use WEP key encrypting. A higher bit key offers better security. WEP encryption scrambles the data transmitted between the wireless stations and the DDW3611 to keep network communications private. It encrypts unicast and multicast communications in a network. Both the wireless stations and the DDW3611 must use the same WEP key. Data Encryption can be set to WEP **128-bit, 64-bit,** or **Disable.**
Shared Key Authentication	Defines Shared Key Authentication as optional or required. Shared Key is an authentication method used by wireless LANs, which follow the IEEE 802.11 standard. Wireless devices authenticate each other by using a secret key that is kept by both devices.
802.1x Authentication	Enables or disables 802.1x to authenticate wireless clients.
Network Key 1-4	Pre-defines up to 4 keys for 64-bit or 128-bit (64-bit keys require 10 hexadecimal digits) (128-bit key require 26 hexadecimal digits).
Current Network Key	Selects one of the four pre-defined keys as the current network key.
Passphrase	Sets the WEP encryption key by entering a word or group of printable characters in the Passphrase box and clicking Generate WEP keys. These characters are case sensitive.
Generate WEP Keys	Forces the device to generate 4 WEP keys automatically.
Automatic Security Configuration — Sets up WPS (Wi-Fi Protected Setup) for devices connecting to the wireless network.	
WPS/Disabled	Enables or disables WPS option. When enabled, the following additional fields are available:
WPS Config State	Defines if the WPS has been configured or not.
Device Name	Defines a name for this wireless cable modem for WPS.

Label	Description
WPS Setup AP	
UUID	Defines the universal unique identifier (UUID) for this access point.
PIN	Defines a randomly generated Personal Identification Number (PIN) for the access point.
WPS Add Client	
Add a client	Activates wireless protected setup (WPS) security on the device. To add a client: 1. Click Add a client. The WPS Add Client screen is displayed. 2. Click PUSH on the WPS Add Client screen.The WPS button is activated on the device, indicated by a flashing white light on top of the unit. 3. Press the WPS button on the device.
Client PIN	Defines a PIN number for client access.
Authorized Client MAC	Defines the MAC address of the authorized client.
Apply	Saves WPS configurations when clicked.

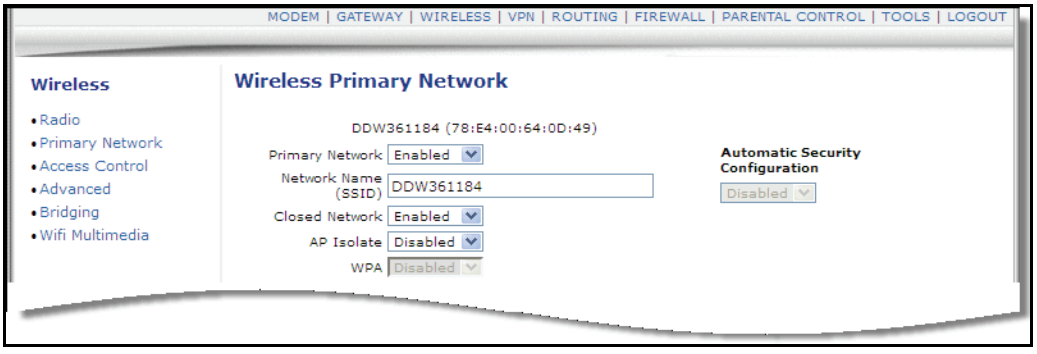
6.2.1 Enabling a Closed Network

You can enable the Closed Network option so the SSID cannot be broadcast or seen by others.

Steps

To enable a closed network:

1. Disable the WPS automatic security configuration.
2. Click **Apply**.
3. Access the pull down menu for the **Closed Network**.
4. Choose **Enabled** to close the network to other users.



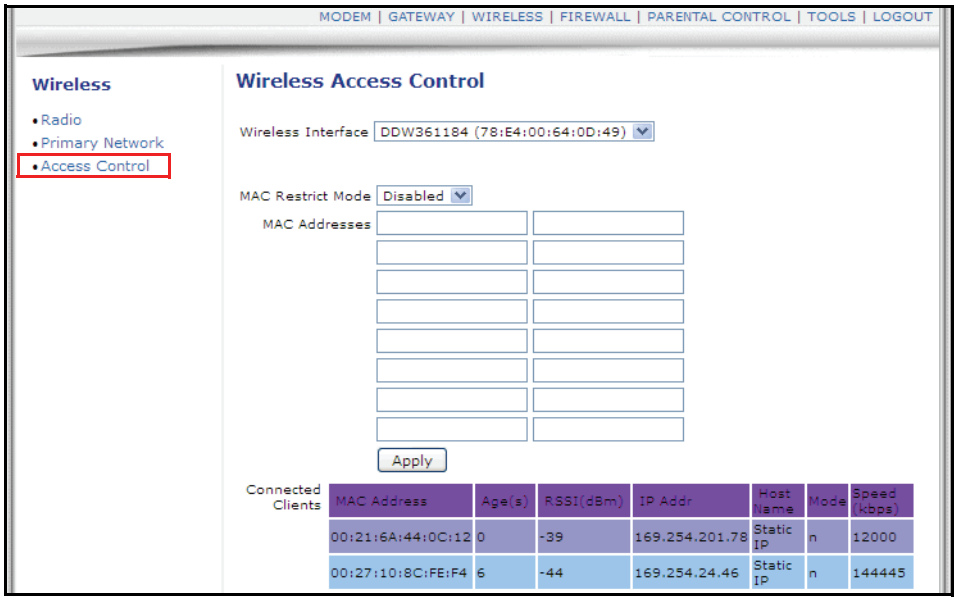
6.3 Using the Access Control Option

The **Access Control** option allows you to configure which clients can access your wireless network.

Steps

To configure client access:

1. Click **Wireless** from the main menu.
2. Click **Access Control** from the left side menu. Field descriptions are listed below the screen example.



Label	Description
Wireless Interface	Defines the network name for which you are setting access control parameters.
MAC Restrict Mode	Controls wireless access to your network by MAC address. ♦ **Disabled** turns off MAC restrictions and allows any wireless client to connect to this device. However, if you use other security mechanisms for access to the wireless network, clients must still adhere to those restrictions. ♦ **Allow** creates a list of wireless clients that can connect to the wireless network. Enter the MAC addresses of these clients in the MAC Addresses fields. MAC addresses not on the list, are not allowed access to your wireless network. ♦ **Deny** creates a list of wireless clients that you do not want to have access to your wireless network. Enter the MAC addresses of these clients in the MAC Addresses fields.

Label	Description
MAC Addresses	Defines the MAC addresses. Note: You may cut and paste MAC addresses from the connected clients list at the bottom of the screen.
Apply	Saves changes when clicked.
Connected Clients	Lists wireless clients currently connected listed by MAC address. ♦ **MAC Address** – Displays the MAC addresses entered in the MAC Addresses field (see above). ♦ **Age(s)** – Displays the duration since the wireless client's polled values were sent to the device. The values include all information shown on this screen. The lower the number, the more current its data. ♦ **RSSI(dBm)** – Displays the received signal strength from the device to the wireless cable modem. This value is commonly used to assist in troubleshooting wireless performance issues. A signal strength between 0dBm and -65dBm is considered optimal. Levels of -66dBm and lower (for example, -70, -80, etc.) have a downward impact on wireless data throughput. Refer to on page 66 for more information. ♦ **IP Address** – Displays the IP address assigned to this wireless client. ♦ **Host Name** – Displays the host name of the wireless client. ♦ **Mode** – Indicates the applicable 802.11a/b/g/n standard used by the connected client device. ♦ **Speed (kbps)** – Displays the maximum theoretical link speed negotiated between the wireless gateway and the client. This does not include the overhead associated with encryption, and so on. For example, actual speeds with WEP encryption enabled are typically less than half of the negotiated link speed.TKIP encryption can also affect performance. AES is the most efficient and secure with the highest throughput possible. You can disable WMM if throughput on some client adaptors is adversely affected.

6.4 Deploying and Troubleshooting the Wireless Network

This section provides the following information to help you understand, deploy, and troubleshoot your wireless environments.

Topics

See the following topics:

6.4.1 Understanding Received Signal Strength

Received signal strength (RSSI) is measured from connected wireless client devices to the wireless cable modem. This value can significantly impact wireless speeds/performance. It is determined by:

- ❑ Materials (for example, open air, concrete, trees)
- ❑ Distance between wireless clients and the wireless cable modem
- ❑ Wireless capabilities of the client devices

To determine the received signal strength, refer to Using the Access Control Option on page 65 and review the **RSSI** value. A receive signal strength indicator between 0 and -64 is considered optimal. Levels of -67dBm and lower (for example, -70, -80, etc.) have a downward impact on wireless data throughput.

6.4.2 Estimating Wireless Cable Modem to Wireless Client Distances

The information in this section helps you to determine how far a wireless cable modem can be placed from wireless client devices. Environmental variances include the capabilities of wireless clients and the types of material through which the wireless signal must pass. When the wireless cable modem and wireless clients reach the distance threshold between each other, network performance degrades.

Steps

To determine wireless cable modem placement:

1. Connect a wireless client to the wireless cable modem. Refer to Connecting Devices to the Network on page 12 if needed.
2. Place the wireless client at around one meter (three feet) away from the wireless cable modem.
3. Obtain the **RSSI** value for the connected client. Refer to Using the Access Control Option on page 65. This value is used in the formula further below.
4. Use the following table to determine what materials the wireless signal must travel through to reach the desired wireless coverage distance.

Attenuation Considerations at 2.4GHz

Material	Attenuation
Connector/Cable	3.5dB
Free Space	.24dB / foot
Interior Drywall	3dB to 4dB
Cubicle Wall	2dB to 5dB
Wood Door (Hollow/Solid)	3dB to 4dB
Brick, Concrete Wall (Note 1)	6dB to 18db

Attenuation Considerations at 2.4GHz

Material	Attenuation
Glass Window (not tinted)	2dB to 3dB
Double Pane Coated Glass	13dB
Bullet Proof Glass	10dB
Steel / Fire Exit Door	13dB to 19dB
Human Body	3dB
Trees (Note 2)	.15dB / foot
Note 1: Different types of concrete materials are used in different parts of the world and the thickness and coating differ depending on whether it is used in floors, interior walls, or exterior walls.	**Note 2**: The attenuation caused by trees varies significantly depending upon the shape and thickness of the foliage.

5. Use the attenuation value from the materials table above in the following formula:

   Formula:

   (Transmit Power, **use -30dBm**) **–** (Receiver Sensitivity, **use RSSI value**) **=** Allowable Free Space Loss

   Allowable Free Space Loss **÷** Materials Attenuation Value **=** Optimal Distance in Feet Between the Cable Modem and a Wireless Client

   Example:

   (-30dBm) **-** (-67dBm) **=** 37dBm (allowable free space loss for a 54Mbps connection)

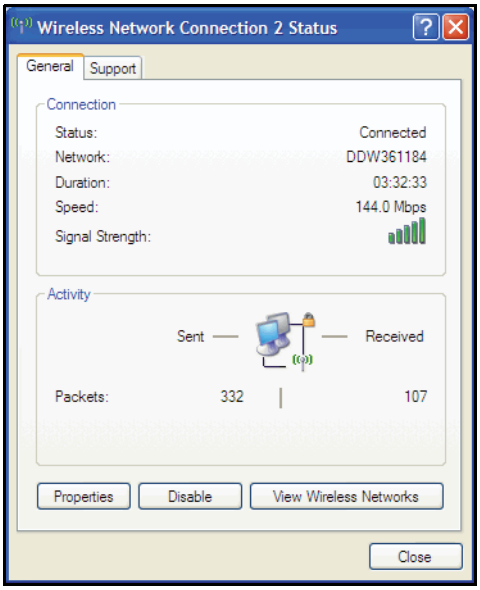
   37dBm **÷** .24db/foot (for open space) **=** 154.16 feet

6. Once you know the optimal feet distance between individual wireless clients and the wireless cable modem, you may resolve and prevent some performance issues.

7. To check the wireless signal strength and speed, use the following steps for a Windows computer connected wirelessly to the wireless cable modem. If the wireless computer is not connected, refer to Connecting a Wireless Device on page 13.

   a. Double-click the Wireless networking icon in the system tray.

b. Review the speed and signal strength in the Status window.



6.4.3 Selecting a Wireless Channel

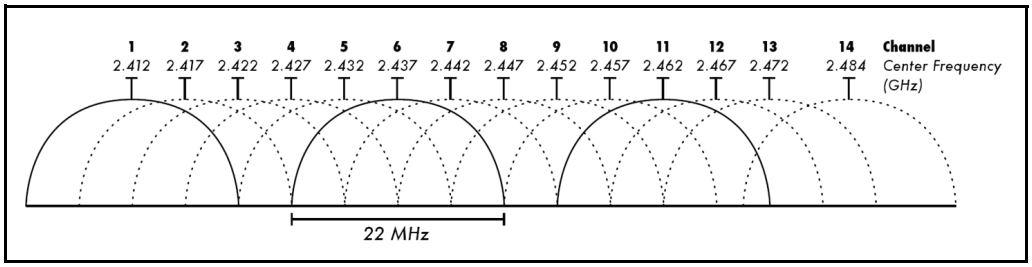
You may need to change the wireless channel on which the wireless cable modem operates when you are in computing, test, and other environments where several wireless access points may be operating in the 2.4Ghz range.

In some cases, you may want to segment your wireless traffic where a group of devices operates on one channel and another group operates on another channel, and so on. This is done by configuring the channel on each wireless access point individually (if you have multiples). If you have control over only one wireless device in an environment where there may be several, you can change the wireless channel on your device to one that is not heavily used.

Note

To change the wireless broadcast channel, refer to Using the Wireless Radio Option on page 57.

The following diagram displays the channels available in the Americas. Each available channel is 22Mhz wide. Since channels overlap, it is best to choose channels that have the least overlap (typically 1, 6, and 11 in the Americas, and 1, 5, 9, and 13 in Europe). Overlapping channels can cause wireless network performance issues.



Note – Source: Wikipedia.org, and IEEE article IEEE 802.11n-2009

7 Understanding the Firewall Menu

This chapter provides instructions to configure the DDW3611 firewall to control what types of traffic are allowed on your network. The firewall can block certain Web-oriented cookies, java scripts, and pop-up windows. It is highly recommended the Firewall is left enabled at all times to protect against denial of service (DoS) attacks. Refer to Using the Basic Option on page 77 to block Internet access to specific sites.

Note

Firewall menu options are not available when the device is in Bridge mode.

Topics

See the following topics:

Steps

To access the firewall menu:

1. Access the Web interface. Refer to Accessing the Web Interface on page 17.
2. Click **Firewall** from the main menu.

7.1 Using the Content Filter Option

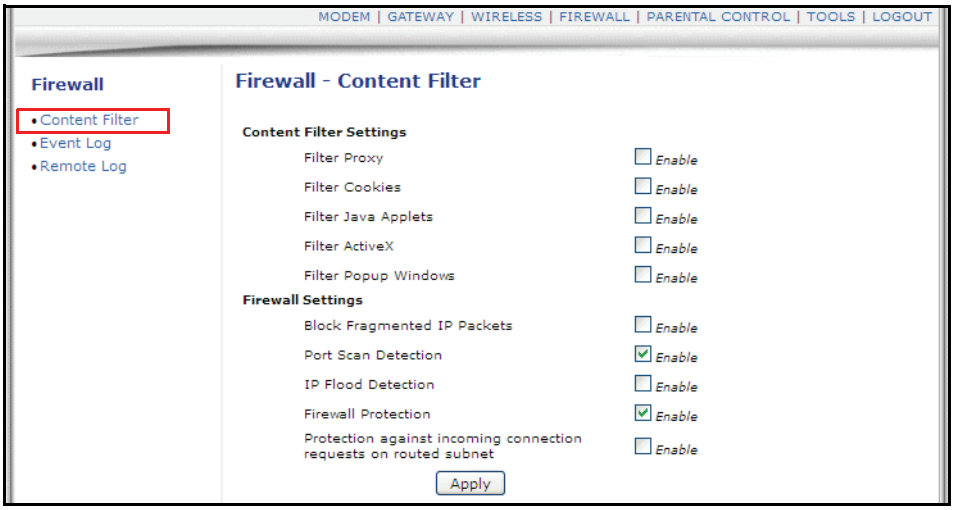
The **Content Filter** option allows you to block certain Web-oriented cookies, java scripts, and pop-up windows.

Steps

To filter Web content:

1. Click **Firewall** from the main menu.
2. Click **Content Filter** from the left side menu. Field descriptions are listed below the

screen example.



Label	Description
Content Filter Settings	
Filter Proxy	Acts as an intermediary between a user and the Internet to provide security, administrative control, and caching service. When a proxy server is located on the WAN, it is possible for LAN users to circumvent content filtering by pointing to this proxy server.
Filter Cookies	Stops Cookies from being stored on a connected computer's hard drive. Some Web servers use them to track usage and provide service based on an ID found in the Cookies.
Filter Java Applets	Stops Java applets from being launched on connected computers. Java is a programming language and development environment for building downloadable Web components or Internet and intranet business applications.
Filter ActiveX	Stops ActiveX applications from being launched on connected computers. ActiveX is a tool for building dynamic and active Web pages and distributed object applications. When you visit an ActiveX Web site, ActiveX controls are downloaded to your browser, where they remain in case you visit the site again.
Filter Popup Windows	Stops popup windows when visiting some Websites.
Firewall Settings	
Block Fragmented IP Packets	Detects fragmented IP packets and blocks them.This option is important for some gaming systems, Vonage TA or other VoIP telephone adaptors.
Port Scan Detection	Detects port scan attacks.
IP Flood Detection	Detects IP flood attacks, which can result in slow web responsiveness due to high packet loss (as much as 90%) due to dropped packets as part of the protection algorithm.

Label	Description
Firewall Protection	Activates the firewall function. Disabling Firewall Protection does NOT disable all other setting; you must enable/disable each one individually as appropriate.
Protection against incoming connection requests on routed subnet	Protects all the routed subnets connected to the device.
Apply	Saves the configuration when clicked.

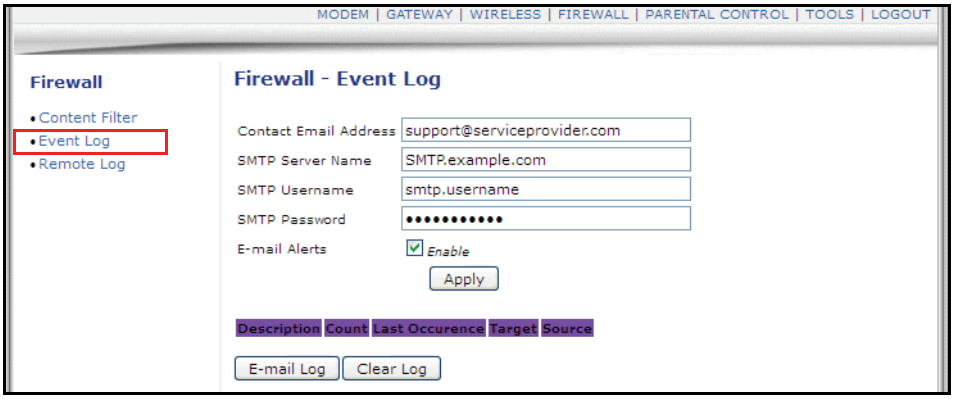
7.2 Using the Event Log Option

The **Event Log** option allows you to configure firewall event log reporting via email alerts and report on possible attacks on the system.

Steps

To configure firewall event reporting:

1. Click **Firewall** from the main menu.
2. Click **Event Log** from the left side menu. Field descriptions are listed below the screen example.



Label	Description
Contact Email Address	Defines the email address where you want to send the log.
SMTP Server Name	Defines the name of the SMTP server, such as smtp.example.com.
SMTP Username	Defines the username for the email address, such as contact@company.com.
SMTP Password	Defines the password for the email address.
E-mail Alerts	Enables or disables event log reporting.

Apply	Saves the settings and completes the setup.
Email Log	Sends the log to the specified email address.
Clear Log	Deletes the log.

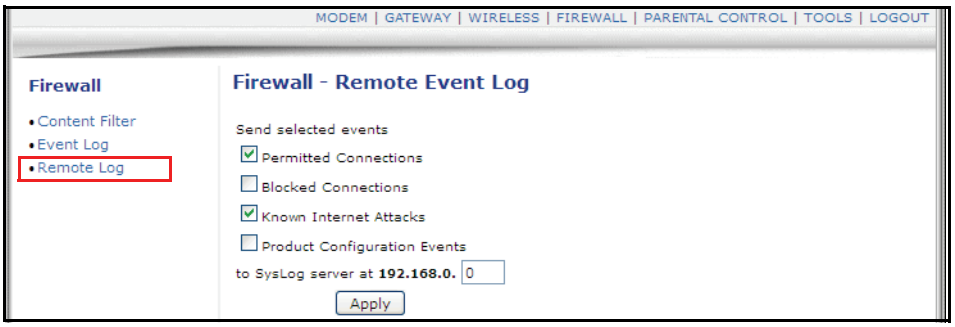
7.3 Using the Remote Log Option

The **Remote Log** option allows you to configure events to be sent to a local SysLog server.

Steps

To configure the firewall remote log:

1. Click **Firewall** from the main menu.
2. Click **Remote Log** from the left side menu. Field descriptions are listed below the screen example.



Label	Description
Permitted Connections	Logs all access attempts that are allowed by the firewall.
Blocked Connections	Logs all access attempts that are blocked by the firewall.
Known Internet Attacks	Logs all known attacks from the Internet.
Product Configuration Events	Logs when the DDW3611 is configured/modified by a user or administrator.
SysLog server	Defines the IP address of the Syslog server.
Apply	Saves the remote log configuration when clicked.

8 Understanding the Parental Control Menu

Parental Controls allow you to control Internet access for users on the DDW3611 network. Parental Controls provides the following features:

- ❑ Define user/password access.
- ❑ Block specific Web sites and Web sites based on keywords.
- ❑ Define the times users are allowed to access the Internet.
- ❑ View an event log to view Internet activity.

Topics

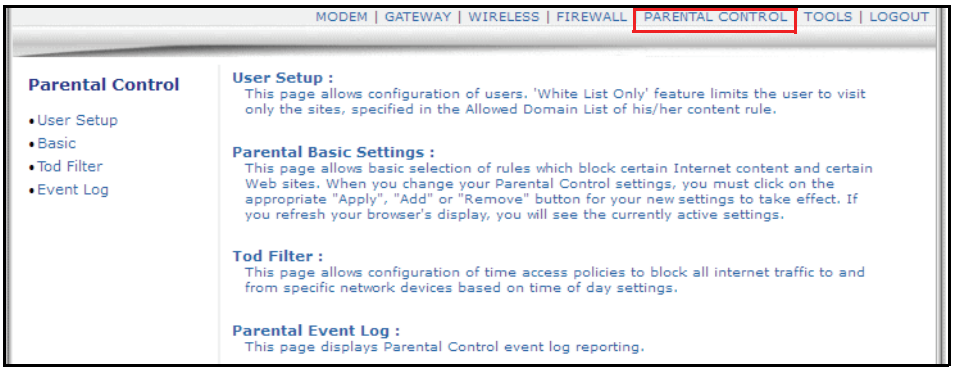
See the following topics:

- ♦ Using the Parental Control User Setup Option on page 75
- ♦ Using the Basic Option on page 77
- ♦ Using the Tod Filter Option on page 79
- ♦ Using the Event Log Option on page 80

Steps

To access the parental control menu:

1. Access the Web interface. Refer to Accessing the Web Interface on page 17.
2. Click **Parental Control** from the main menu.



8.1 Using the Parental Control User Setup Option

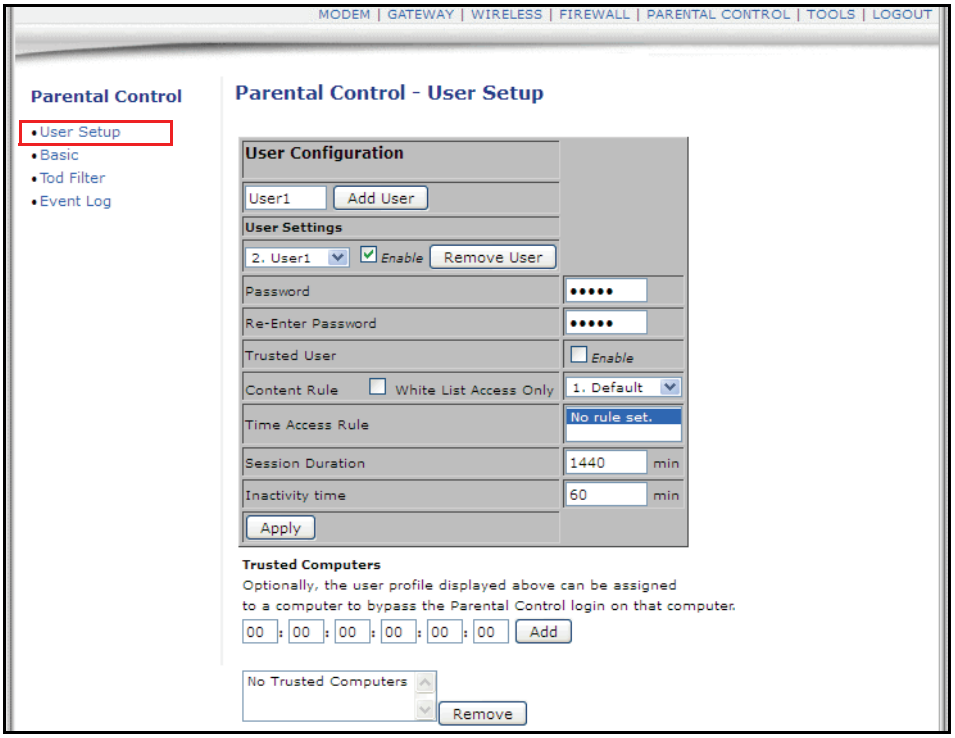
The **User Setup** option allows you to configure which user accounts can or cannot connect to your wireless or wired network, and the parameters of each connection.

Steps

To configure user accounts:

1. Click **Parental Control** from the main menu.
2. Click **User Setup** from the left side menu. Field descriptions are listed below the screen example.

   Note: To enable Parental Control, refer to Using the Basic Option on page 77.



Label	Description
Add User **Remove User** **Enable**	Defines user accounts. ♦ To select an existing user, choose the user from the User Settings pop-up menu. ♦ To add a new user, add the user name and click Add. ♦ To activate the user, check Enable. ♦ To remove a user, select the user from the pop-up menu and click Remove User.
Password	Defines the password for this user. It is required when this user tries to access the Internet via the device.
Re-Enter Password	Checks the password with the re-entered password.
Trusted User	Defines the selected user as a trusted user when enabled is checked. The user is limited to timing and content when visiting the Internet, as defined in the following fields.
Content Rule	Selects from the pop-up menu an existing content rule that defines what kind of Websites the user can visit or not.

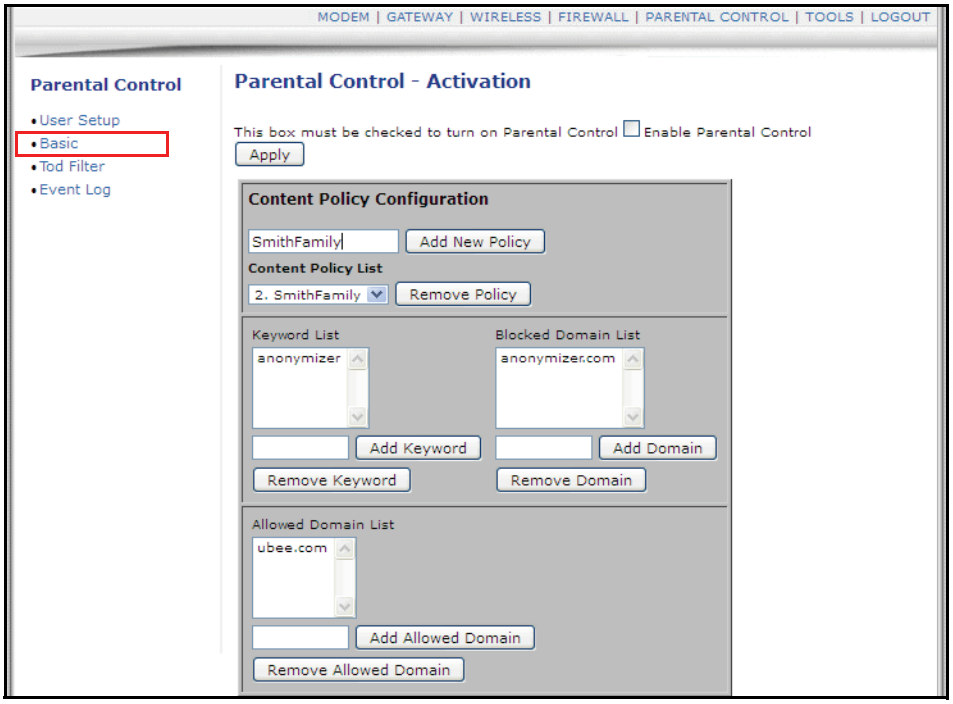
Label	Description
White List Access Only	Selects the White List Access option. If you have created a content rule that defines a black list and white list, select the White List Access Only checkbox to force the wireless modem to execute the policy for the selected user.
Time Access Rule	Selects a defined time access rule to apply to the selected user.
Session Duration	Allows you to enter a time in minutes for the user's session to expire. When the session expires, the user can log in again for the same session duration.
Inactivity Time	Allows you to enter the time out value when a user has no activity on the Internet. When the time expires, the user interface to the Internet is cancelled.
Apply	Saves all changes when clicked.
Trusted Computers	Defines the trusted hosts that can bypass the Parental Control Process.
Add	Adds the trusted host's MAC address entered in the given area and Add is clicked.
Remove	Removes a trusted computer from the list when it is highlighted and Remove is clicked.

8.2 Using the Basic Option

The **Basic** option allows you to select rules to block certain Internet content and Web sites. After you change your Parental Control settings, click the appropriate Apply, Add, or Remove button for your new settings to take effect. Refresh your browser's display to see the currently active settings.

To filter Internet content and Web sites:

1. Click **Parental Control** from the main menu.
2. Click **Basic** from the left side menu. Field descriptions are listed below the screen example.



Label	Description
Enable Parental Control	Activates the Parental Control feature when checked.
Apply	Saves all changes in the screen and activates Parental Control, if enabled.
Content Policy Configuration	
Add New Policy	Adds a policy to the Policy List. Enter the policy name and click Add New Policy.
Content Policy List	Lists existing policies you can choose to use.
Remove Policy	Deletes a policy from the list. Select the policy from the list and click Remove Policy.
Keyword List	Displays keywords you can use to block Web site addresses (URLs) containing those words.
Add Keyword	Adds a keyword to the keyword list. Enter the word in the field next to the Add Keyword button and click Add Keyword. The keyword is added to the list.
Remove Keyword	Removes a keyword from the keyword list. Select the keyword from the list, and click Remove Keyword.
Blocked Domain List	Displays Web domains (for example, unwanted.com) you can use to block access to those domains.
Add Domain	Adds a domain to the Allowed Domain List. Enter a domain, and click Add Domain.
Remove Allowed Domain	Removes a domain from the Allowed Domain List. Select the domain from the list, and click Remove Domain.

Label	Description
Allowed Domain List	DIsplays domains you can assign to users to visit only the sites allowed.
Add Allowed Domain	Adds allowed domains to the list. Enter the name and click Add Allowed Domain.
Remove Allowed Domain	Removes domain names from the list. Highlight the domain from the list and click Remove Allowed Domain.

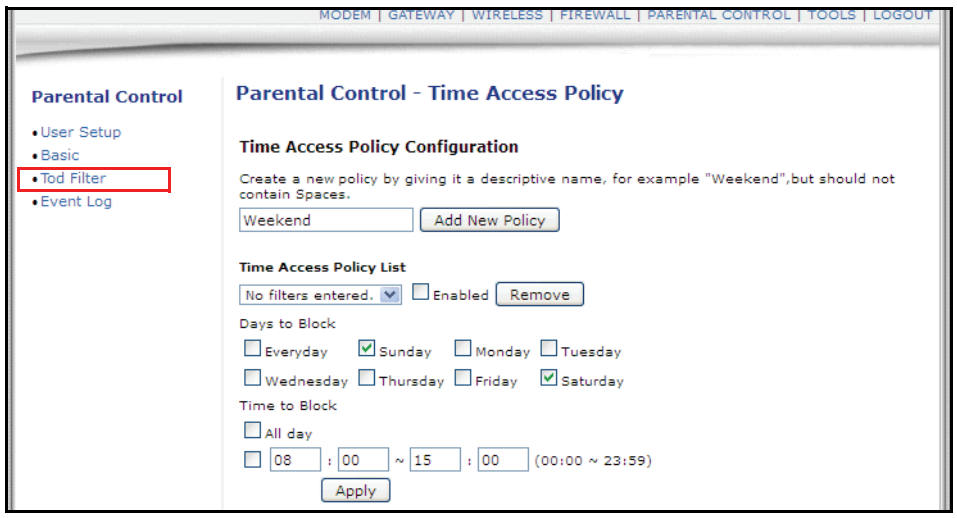
8.3 Using the Tod Filter Option

The **Tod Filter** option allows the configuration of time-based access policies to block all Internet traffic at specified times.

Steps

To configure time-of-day filters:

1. Click **Parental Control** from the main menu.
2. Click **Tod Filter** from the left side menu. Field descriptions are listed below the screen example.



Label	Description
Add New Policy	Adds a new policy. Enter a policy name and click the Add New Policy button.
Time Access Policy List	Lists the existing policies in a drop-down list.
Enabled	Activates a policy. Select the policy from the drop-down list and check Enabled.
Remove	Deletes a policy. Select the policy from the drop-down list and click Remove.

Label	Description
Days to Block	Selects the days to block Internet access.
Time to Block: **All Day or by Start and End Time**	Defines the time to block. ♦ To block all day, check All Day to eliminate all access during the days selected. ♦ To block specific times, enter the time range in the Start and End fields.
Apply	Saves all changes when clicked.

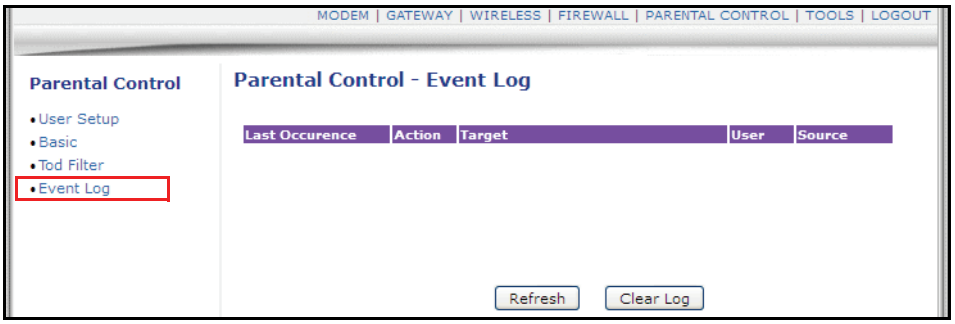
8.4 Using the Event Log Option

The **Event Log** option displays Parental Control event log reporting.

Steps

To view the parental control event log:

1. Click **Parental Control** from the main menu.
2. Click **Event Log** from the left side menu. Field descriptions are listed below the screen example.



Label	Description
Last Occurrence	Displays the time when the last event occurred.
Action	Displays what is done by parental control, including dropping or permitting access requests.
Target	Displays the destination IP address of a certain access request.
User	Displays the user who triggered this event log.
Source	Displays the source IP address of this event.
Refresh/Clear Log	Displays the event log. ♦ To update the log with the most current events, click Refresh. ♦ To empty the displayed log entries, click Clear.

9 Understanding the Tools Menu

This chapter instructs you how to use a variety of tools to evaluate and diagnose the DDW3611.

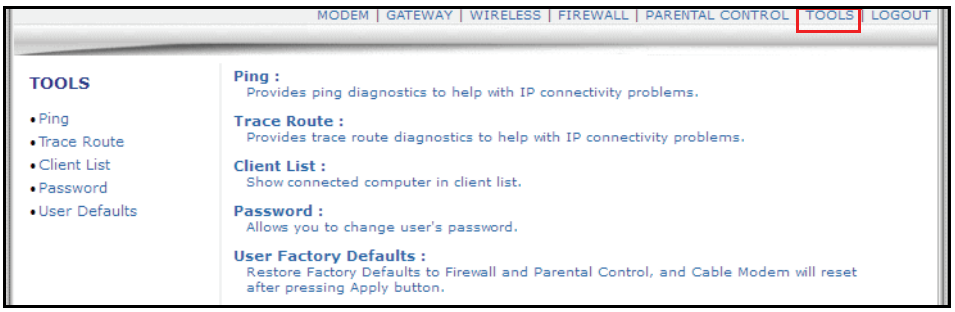
Topics

See the following topics:

Steps

To access the tools menu:

1. Access the Web interface. Refer to Accessing the Web Interface on page 17.
2. Click **Tools** from the main menu.



9.1 Using the Ping Option

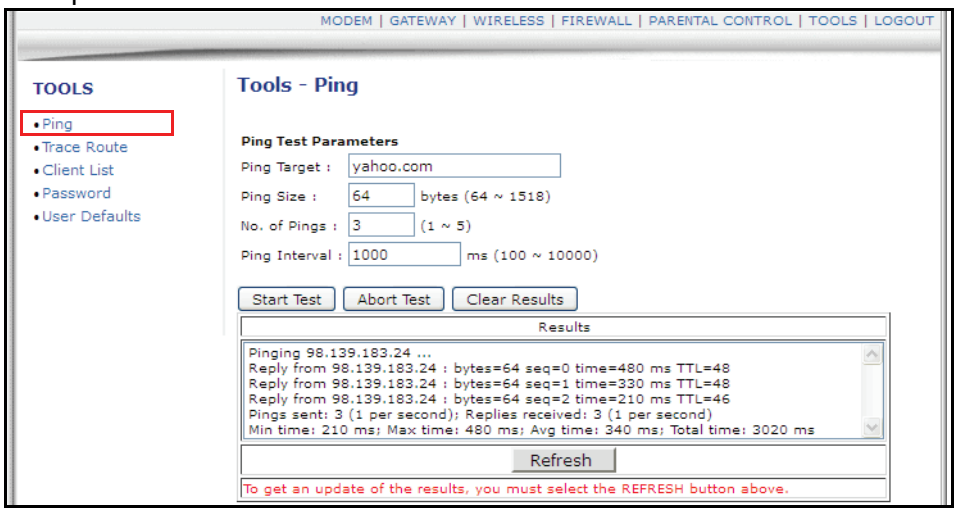
The **Ping** utility tests the network connectivity between devices by sending a test message to a specific device. You can also confirm the size of data sent is the same as the size of data received.

Steps

To test connectivity between devices:

1. Click **Tools** from the main menu.
2. Click **Ping** from the left side menu. Field descriptions are listed below the screen

example.



Label	Description
Ping Test Parameters	
Ping Target	Defines the IP address to which you want to send a ping.
Ping Size	Defines the packet size to send for the ping operation.
No. of Pings	Defines the number of ping commands to send to the ping target.
Ping Interval	Defines the interval between ping operations in milliseconds.
Start Test/Abort Test/Clear Results	Defines what you want to do. ♦ To start the test, click Start Test ♦ To cancel the test, click Abort Test. ♦ To clear the displayed results, click Clear Results.
Results	Displays the results of the ping test.
Refresh	Updates the results in the Results window. You must click the Refresh button to get the latest results.

9.2 Using the Trace Route Option

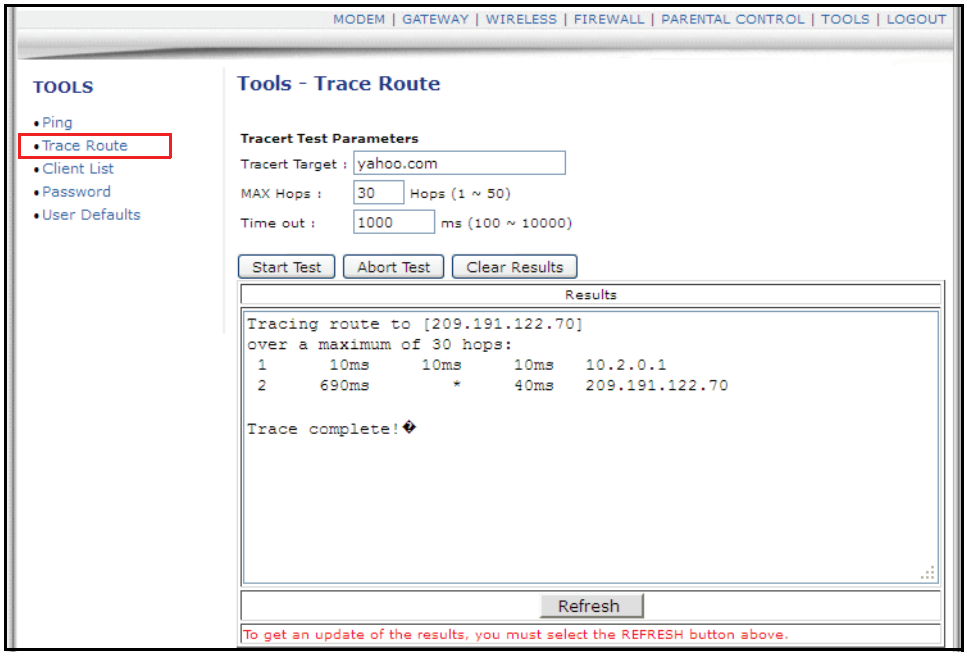
The Trace Route utility determines the IP addresses of the hosts on the path. By checking the Resolve host names box, Trace Route tries to find which name matches the address. Some hosts have no names, and might still be shown as IP addresses, even if this option is active.

Steps

To trace host IP addresses along a route:

1. Click **Tools** from the main menu.
2. Click **Trace Route** from the left side menu. Field descriptions are listed below the

screen example.



Label	Description
Tracert Test Parameters	
Tracert Target	Defines the specific IP address or domain (for example, yahoo.com) to which you want to trace a route.
MAX Hops	Defines the MAX hops. Hops is the number of routers that the trace route traverses.
Time out	Defines the time out interval (100–10000) in milliseconds.
Start Test **Abort Test** **Clear Results**	Defines what you want to do. ♦ To start the test, click Start Test. ♦ To cancel the test, click Abort Test. ♦ To clear the displayed results, click Clear Results.
Results	Displays the results of the test. Once the traceroute is complete, an ordered list of hosts is displayed, the number of times the host answered, and how fast the host answered the probes.
Refresh	Updates the results in the Results window. You must click the Refresh button to get the latest results.

9.3 Using the Client List Option

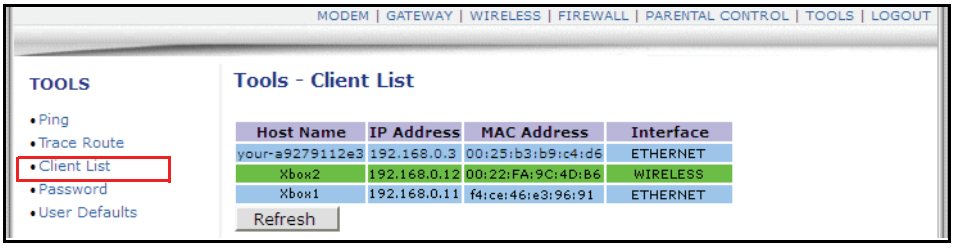
The **Client List** option displays computers connected to the DDW3611.

Steps

To view a list of computers connected to this device:

1. Click **Tools** from the main menu.
2. Click **Client List** from the left side menu. Field descriptions are listed below the screen example.

   Note – Devices connected with an IPv6IP address are shown in the Gateway Setup LAN IPv6 screen.



Label	Description
Hostname	DIsplays the hostname of the DHCP clients connected to the DDW3611.
IP Address	DIsplays the IP address of the DHCP clients connected to the DDW3611.
MAC Address	DIsplays the MAC address of the DHCP clients connected to the DDW3611.
Interface	Displays how clients are connected to the device, for example, ethernet LAN, Wireless.
Refresh	Refreshes the client list. This may be useful when testing network connectivity between connecting clients and the DDW3611.

Field descriptions are listed below the screen example

9.4 Field descriptions are listed below the screen example Using the Password Option

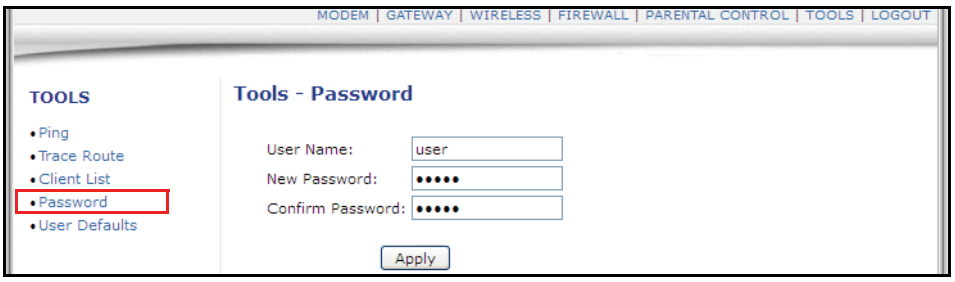
The **Password** option allows you to change the password for the **user** login on the DDW3611. This login is used to access this Web interface.

Steps

To change the password for the user login:

1. Click the **Tools** link from the top of the screen.

2. Click **Password** from the left side of the screen. The **Password** fields are explained following this screen example.



Label	Description
User Name	Allows you to enter a new user name for the **user** account to this Web interface of the DDW3611. See Understanding Default Values and Logins on page 7 for more information on logins and defaults. Enter the new Password and re-enter the new password to confirm. Click Apply to save the changes.
New Password	Allows you to enter a new password for the user account.
Confirm Password	Allows you to re-enter the new password to confirm.
Apply	Saves all changes when clicked.

Field descriptions are listed below the screen example

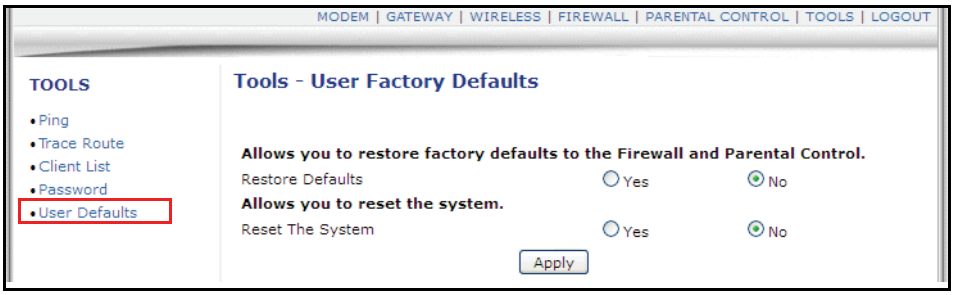
9.5 Using the User Defaults Option

The **User Defaults** option allows you to restore factory defaults to the Firewall and Parental Control settings. All other networking setting are not cleared and reset (for example, wireless settings).

Note

Restoring factory defaults to the system resets the user login/password to the device. Refer to Understanding Default Values and Logins on page 7 for the default values.

1. Click the **Tools** link from the top of the screen.
2. Click **User Defaults** from the left side of the screen. The **User Defaults** fields are explained following this screen example.



Label	Description
Restore Factory Defaults to Firewall and Parental Control	Restores settings to factory defaults. Select Yes to restore the device to default settings for the Firewall and Parental Control settings. This operation does not require a reset of the system.
Reset The system	Resets the system. Select Yes to power cycle the device.
Apply	Applies the options selected in this screen.

Field descriptions are listed below the screen example

10 Glossary

This chapter defines terms used in this guide and in the industry.

Broadcast
A packet sent to all devices on a network.

Cable Modem Termination System (CMTS)
Typically located in the cable company's headend, the CMTS is equipment that provides high-speed data services to subscribers, such as cable Internet and VoIP.

Channel Bonding
A computer networking configuration where two or more network interfaces are combined on a host computer for redundancy or increased throughput. Data is transmitted over these channels as if they are one channel.

Customer Premises Equipment (CPE)
Equipment such as telephones, routers, and modems located at a subscribers location to enable customers access to communication services.

Default Gateway
The routing device used to forward all traffic that is not addressed to a computer on the local subnet.

Demilitarized Zone (DMZ)
Allows one IP address (or computer) to be placed in between the firewall and the Internet (usually for gaming and video conferencing). This allows risky, open access to the Internet.

Domain
A subnetwork comprised of a group of clients and servers under the control of one security database.

Domain Name
A descriptive name for an address or group of addresses on the Internet. Domain names are in the form of a registered entity name plus one of a number of predefined top-level suffixes, such as .com, .edu, .org.

Domain Name System (DNS)
An Internet service that locates and translates domain names into IP addresses. Because domain names are alphabetic, they are easier to remember. However, the Internet is based on IP addresses. Every time you use a domain name, a DNS service translates the name into the corresponding IP address. The DNS system is actually its own network. If one DNS server does not know how to translate a particular domain name, it asks another one, and so on, until the correct IP address is returned.

Downstream
A term to describe the direction of data from the network service provider to the customer.

Dynamic Host Configuration Protocol (DHCP)
A protocol that centrally automates the assignment of IP addresses in a network. Using the Internet's set of protocols (TCP/IP), each machine that can connect to the Internet needs a unique IP address. For example, when the service provider sets up computer users with a connection to the Internet, an IP address is assigned to each machine. DHCP lets the service provider distribute IP addresses and automatically sends a new IP address when a computer is plugged in to the high-speed Internet network. DHCP uses the concept of a "lease" or amount of time an IP address is valid for a computer. Lease times can vary.

Ethernet
A standard network protocol that specifies how data is placed on and retrieved from a common transmission medium. It forms the underlying transport vehicle used by several upper-level protocols, including TCP/IP and XNS.

Firewall
A highly effective method to block unsolicited traffic from outside the connected computers in your gateway.

Gateway
A local device, usually a router, that connects hosts on a local network to other networks – sometimes with different incompatible communication protocols.

Headend
A main facility to process and distribute Internet communication signals. Headend may also refer to cable television signals and power line communication facilities.

Internet Protocol (IP)
The method or protocol by which data is sent from one computer to another on the Internet. It is a standard set of rules, procedures, or conventions relating to the format and timing of data transmission between two computers that they must accept and use to understand each other. Used in conjunction with the Transfer Control Protocol (TCP) to form TCP/IP.

IP Address
In the most widely installed level of the IP today, an IP address is a 32-bit binary digit number that identifies each sender or receiver of information that is sent in packet form across the Internet. When you request a Web page or send an e-mail, the IP part of TCP/IP includes your IP address. IP sends your IP address to the IP address obtained by looking up the domain name in the URL you requested or in the e-mail address to which you are sending a note. A dynamic IP address is an IP address that is automatically assigned to a client station in a TCP/IP network, typically by a DHCP server.

Internet Service Provider (ISP)
A company that provides individuals and companies access to the Internet and other related services.

Interval Usage Code (IUC)
Interval usage codes define different profiles for upstream burst profiles to use for the data. IUCs are sent to the cable modem from the CMTS to tell the device important characteristics to use for the burst, such as modulation type, preamble length, and so on.

Local Area Network (LAN)
A group of computers and associated devices such as printers and servers that share a common communication line and other resources within a small geographic area.

Media Access Control (MAC) Address
A unique number assigned by the manufacturer to any Ethernet networking device, such as a network adapter, that allows the network to identify it at the hardware level. Usually written in the form 01:23:45:67:89:ab.

Megabits per Second (Mbps)
A unit of measurement for data transmission that represents one million bits per second.

Maximum Transmission Unit (MTU)
The size in bytes of the largest packet that can be sent or received.

Network Address Translation (NAT)
A technique by which several hosts or computers share a single IP address for access to the Internet. NAT enables a LAN to use one set of IP addresses for internal traffic and a second set of addresses for external traffic, and provides a type of firewall by hiding internal IP addresses.

Network Basic Input Output System (NetBIOS)
An application programming interface (API) that augments the DOS BIOS by adding special functions for LANs. Almost all Windows-based LANs for PCs are based on the NetBIOS.

Network Operations Center (NOC)
A location that controls computer, television, or telecommunications networks. Large organizations usually have more than one network operations center to manage multiple networks.

Packet
A block of information sent over a network. A packet typically contains a source and destination network address, some protocol and length information, a block of data, and a checksum.

Ranging
A process in which a cable modem sends a range request at a power of 8 dBmV (very low power). If it does not rec i eve a range response from the CMTS, the cable modem re-transmits the range request at a 3 dB higher power level and continues the process until a range response is received.

Routing Information Protocol (RIP)
A protocol in which routers periodically exchange information with one another to determine minimum-distance paths between sources and destinations.

Router
A device that forwards data between networks. An IP router forwards data based on IP source and destination addresses.

Subnet
A portion of a network that shares a common address component. On TCP/IP networks, subnets are defined as all devices whose IP addresses have the same prefix. For example, all devices with IP addresses that start with 10.1.10 would be part of the same subnet. IP networks are divided using a subnet mask.

Subnet Mask
Combined with the IP address, the IP subnet mask allows a device to know which other addresses are local to it, and which must be reached through a gateway or router. A number that explains which part of an IP address comprises the network address and which part is the host address on that network.

Telnet
A network protocol used on the Internet or a local area network. Provides bi-directional interactive text-oriented communications using a virtual terminal connection.

Terminal Access Controller Access-Control System (TACACS)
A remote authentication protocol used to communicate with an authentication server to determine if the user is allowed to access the network.

Time Division Multiple Access (TDMA)
A method in which cable modems must time-share the upstream channel because there are many cable modems and only one upstream channel frequency.

Transmission Control Protocol (TCP)
A method (protocol) used with the IP to send data in the form of message units (datagrams) between network devices over a LAN or WAN. While IP handles the actual delivery of the data (routing), TCP keeps track of the individual units of data (packets) that a message is divided into for efficient delivery over the network. TCP requires the receiver of a packet to return an acknowledgment of receipt to the sender of the packet.

Transmission Control Protocol/Internet Protocol (TCP/IP)
The basic communication language or set of protocols to communicate over a network (developed specifically for the Internet). TCP/IP defines a suite or group of protocols.

Trivial File Transfer Protocol
A file transfer protocol used to transfer automatically configuration or boot files.

Uniform Resource Identifier (URI)
A string of characters used to identify a name or a resource on the Internet.

Upstream
A term to describe the direction of data from the customer to the network service provider.

Uniform Resource Locator (URL)
A URI that specifies where a known resource is available and how to retrieve it.

Wide Area Network (WAN)
A long-distance link or computer network that spans a relatively large geographical area that connects remotely located LANs. Typically, a WAN consists of two or more LANs. The Internet is a large WAN.

Wi-Fi Protected Setup (WPS)
A security protocol for wireless home networks. Created by the Wi-Fi Alliance, this protocol allows home users to easily set up wireless security and add new devices without needing to enter long passwords.

Wireless Local Area Network (WLAN)
A method that links two or more devices to provide a connection through an access point the wider Internet. Users can move within the local coverage area and stay connect to the network.

Xerox Network Services (XNS)
A protocol suite developed by Xerox that provides general purpose network communications, Internet routing, and packet delivery.